ETSI TS 129 061 V4.9.0 (2003-12)

Technical Specification

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
Interworking between the Public Land Mobile Network (PLMN)
supporting packet based services and
Packet Data Networks (PDN)
(3GPP TS 29.061 version 4.9.0 Release 4)**



Reference
RTS/TSGN-0329061v490

Keywords
GSM, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2003.
All rights reserved.

DECT™, **PLUGTESTS**™ and **UMTS**™ are Trade Marks of ETSI registered for the benefit of its Members.
TIPHON™ and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp .

Contents

Intellectual Property Rights 2
Foreword 2
Foreword 5
1 Scope 6
2 References 6
3 Definitions, abbreviations and symbols 8
3.1 Definitions 8
3.2 Abbreviations 8
3.3 Symbols 9
4 Network characteristics 9
4.1 Key characteristics of PLMN 9
4.2 Key characteristics of PSDN 9
4.3 Key characteristics of IP Networks 10
5 Interworking Classifications 10
5.1 Service Interworking 10
5.2 Network Interworking 10
5.3 Numbering and Addressing 10
6 Access reference configuration 10
7 Interface to Packet Domain Bearer Services 10
7.1 GSM 10
7.2 UMTS 11
8 Subscription checking 11
9 Message Screening 11
10 Interworking with PSDN (X.75/X.25) 12
11 Interworking with PDN (IP) 12
11.1 General 12
11.2 PDN Interworking Model 12
11.2.1 Access to Internet, Intranet or ISP through Packet Domain 13
11.2.1.1 Transparent access to the Internet 14
11.2.1.2 IPv4 Non Transparent access to an Intranet or ISP 15
11.2.1.3 IPv6 Non Transparent access to an Intranet or ISP 17
11.2.1.3.1 IPv6 PDP Context Activation 18
11.2.1.3.2 IPv6 Stateless Address Autoconfiguration 22
11.2.1.3.3 IPv6 Stateful Address Autoconfiguration 23
11.2.1.3.4 IPv6 Router Configuration Variables in the GGSN 24
11.2.1.4 Access to Internet, Intranet or ISP with Mobile IPv4 25
11.3 Numbering and Addressing 28
11.4 Charging 28
11.5 Domain Name System Server (DNS Server) 28
11.6 Screening 28
11.7 IP Multicast access 28
12 Interworking with PDN (PPP) 29
12.1 General 29
12.2 PDN Interworking Model 29
12.2.1 Virtual dial-up- and direct Access to PDNs, or ISPs through Packet Domain 30
12.2.1.1 Procedural description 31
13 Interworking with PDN (DHCP) 32
13.1 General 32

13.2 PDN Interworking Model for DHCP....33
13.2.1 Address allocation by the Intranet or ISP....33
13.2.1.1 Address allocation using DHCPv4....34
13.2.1.2 Address allocation using DHCPv6....35
13.2.2 Other configuration by the Intranet or ISP (IPv6 only)....37

14 Internet Hosted Octet Stream Service (IHOSS)....38

15 Interworking between Packet Domains....38
15.1 Security Agreements....39
15.2 Routing protocol agreements....39
15.3 Charging agreements....40

16 Usage of RADIUS on Gi interface....40
16.1 RADIUS Authentication....40
16.2 RADIUS Accounting....40
16.3 Authentication and accounting message flows....41
16.3.1 IP PDP type....41
16.3.2 PPP PDP type....42
16.3.3 Accounting Update....44
16.3.4 AAA-Initiated PDP context termination....45
16.4 List of RADIUS attributes....45
16.4.1 Access-Request message (sent from the GGSN to AAA server)....45
16.4.2 Access-Accept (sent from AAA server to GGSN)....46
16.4.3 Accounting-Request START (sent from GGSN to AAA server)....47
16.4.4 Accounting Request STOP (sent from GGSN to AAA server)....48
16.4.5 Accounting Request ON (optionally sent from GGSN to AAA server)....50
16.4.6 Accounting Request OFF (optionally sent from GGSN to AAA server)....50
16.4.7 Sub-attributes of the 3GPP Vendor-Specific attribute....51
16.4.8 Accounting Request Interim-Update (sent from GGSN to AAA server)....60
16.4.9 Disconnect Request (optionally sent from AAA server to GGSN)....61

Annex A (informative): Interworking PCS1900 with PSDNs....62

Annex B (informative): Change history....63

History....64

Foreword

This Technical Specification (TS) has been produced by the 3rd Generation Partnership Project (3GPP).

The present document describes the network interworking for the Packet Domain. Interworking to various external networks is defined together with the interworking for data forwarding while subscribers roam within the 3GPP system.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 1 presented to TSG for information;
 - 2 presented to TSG for approval;
 - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines the requirements for Packet Domain interworking between a:

a) PLMN and PDN;

b) PLMN and PLMN.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] Void.

[2] 3GPP TS 22.060: "General Packet Radio Service (GPRS); Service Description; Stage 1 ".

[3] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[4] 3GPP TS 03.61: "Point-to-Multipoint Multicast Service Description; Stage 2".

[5] 3GPP TS 03.62: "Point-to-Multipoint Group Call Service Description; Stage 2".

[6] 3GPP TS 03.64: "General Packet Radio Service (GPRS); Overall description of the GPRS radio interface; Stage 2".

[7] 3GPP TS 04.60: "General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control / Medium Access Control (RLC/MAC) protocol".

[8] 3GPP TS 04.64: "General Packet Radio Service (GPRS); Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) layer specification".

[9] 3GPP TS 24.065: "General Packet Radio Service (GPRS); Mobile Station (MS) - Serving GPRS Support Node(SGSN); Subnetwork Dependent Convergence Protocol (SNDCP)".

[10] 3GPP TS 27.060: "Packet Domain; Mobile Station (MS) supporting Packet Switched Services".

[11] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[12] Void.

[13] Void.

[14] Void.

[15] IETF RFC 768 (1980): "User Datagram Protocol" (STD 6).

[16] IETF RFC 791 (1981): "Internet Protocol" (STD 5).

[17] IETF RFC 792 (1981): "Internet Control Message Protocol" (STD 5).

[18] IETF RFC 793 (1981): "Transmission Control Protocol" (STD 7).

[19] IETF RFC 1034 (1987): "Domain names - concepts and facilities" (STD 7).

[20] Void.

[21a] IETF RFC 1661 (1994): "The Point-to-Point Protocol (PPP)" (STD 51).

[21b] IETF RFC 1662 (1994): "PPP in HDLC-like Framing".

[22] IETF RFC 1700 (1994): "Assigned Numbers" (STD 2).

[23] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

[24] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[25] IETF RFC 2794 (2000): "Mobile IP Network Address Identifier Extension for IPv4", P. Calhoun, C. Perkins.

[26] IETF RFC 2131 (1997): "Dynamic Host Configuration Protocol".

[27] IETF RFC 1542 (1993): "Clarification and Extensions for the Bootstrap Protocol".

[28] IETF RFC 2373 (1998): "IP Version 6 Addressing Architecture".

[29] IETF RFC 2462 (1998): "IPv6 Stateless Address Autoconfiguration".

[30] IETF RFC 2002 (1996): "IP Mobility Support", C. Perkins.

[31] IETF RFC 2486 (1999): "The Network Access Identifier", B. Aboba and M. Beadles.

[32] IETF RFC 1112 (1989): "Host extensions for IP multicasting", S.E. Deering.

[33] IETF RFC 2236 (1997): "Internet Group Management Protocol, Version 2", W. Fenner.

[34] IETF RFC 2362 (1998): "Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification", D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei.

[35] IETF RFC 1075 (1988): "Distance Vector Multicast Routing Protocol", D. Waitzman, C. Partridge, S.E. Deering.

[36] IETF RFC 1585 (1994): "MOSPF: Analysis and Experience", J. Moy.

[37] IETF RFC 2290 (1998): "Mobile-IPv4 Configuration Option for PPP IPCP", J. Solomon, S. Glass.

[38] IETF RFC 2865 (2000): "Remote Authentication Dial In User Service (RADIUS)", C. Rigney, S. Willens, A. Rubens, W. Simpson.

[39] IETF RFC2866 (2000): "RADIUS Accounting", C. Rigney, Livingston.

[40] 3GPP TS 23.003: "Numbering, addressing and identification".

[41] IETF RFC 2882 (2000): "Network Access Servers Requirements: Extended RADIUS Practices", D. Mitton.

[42] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[43] Void.

[44] IETF RFC 2461 (1998): "Neighbor Discovery for IP Version 6 (IPv6)", T. Narten, E. Nordmark, W. Simpson.

[45] IETF RFC 3118 (2001): "Authentication for DHCP Messages", R. Droms, W. Arbaugh.

[46] IETF RFC 3315 (2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney.

[47] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".

[48] IETF RFC 2710 (1999): "Multicast Listener Discovery (MLD) for IPv6", S. Deering, W. Fenner, B. Haberman.

[49] IETF RFC 2460 (1998): "Internet Protocol, Version 6 (IPv6) Specification", S.Deering,, R.Hinden.

[50] IETF RFC 3162 (2001): "RADIUS and IPv6", B. Adoba, G. Zorn, D. Mitton.

[51] IETF RFC 2548 (1999): "Microsoft Vendor-specific RADIUS Attributes", G.Zorn.

[52] IETF RFC 1035 (1987): "Domain names - implementation and specification".

[53] IETF RFC 1771 (1995): "A Border Gateway Protocol 4 (BGP-4)".

[54] IETF RFC 1825 (1995): "Security Architecture for the Internet Protocol".

[55] IETF RFC 1826 (1995): "IP Authentication Header".

[56] IETF RFC 1827 (1995): "IP Encapsulating Security Payload (ESP)".

[57] IETF RFC 2044 (1996): "UTF-8, a transformation format of Unicode and ISO 10646".

[58] 3GPP TS 24.008: “Mobile radio interface layer 3 specification; Core Network Protocols - Stage 3”.

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TS 22.060 [2] and 3GPP TS 23.060 [3] and the following apply:

2G- / 3G-: prefixes 2G- and 3G- refers to functionality that supports only GSM GPRS or UMTS, respectively, e.g. 2G-SGSN refers only to the GSM GPRS functionality of an SGSN. When the prefix is omitted, reference is made independently from the GSM GPRS or UMTS functionality.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

APN	Access Point Name
ATM	Asynchronous Transfer Mode
BG	Border Gateway
CHAP	Challenge Handshake Authentication Protocol
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name System
DVMRP	Distance Vector Multicast Routing Protocol
GGSN	Gateway GPRS Support Node
GTP-U	GPRS Tunnelling Protocol for user plane
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol (PPP NCP for IPv4)
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IPv6 Control Protocol (PPP NCP for IPv6)
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAC	L2TP Access Concentrator
LAN	Local Area Network

LNS	L2TP Network Server
MIP	Mobile IP
MLD	Multicast Listener Discovery
MOSPF	Multicast Open Shortest Path First
MS	Mobile Station
MT	Mobile Terminal
MTU	Maximum Transfer Unit
NAI	Network Access Identifier
PAP	Password Authentication Protocol
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDU	Protocol Data Unit
PIM-SM	Protocol Independent Multicast – Sparse Mode
PPP	Point-to-Point Protocol
PS	Packet Switched
RADIUS	Remote Authentication Dial In User Service
SGSN	Serving GPRS Support Node
SMDS	Switched Multimegabit Data Service
TCP	Transmission Control Protocol
TE	Terminal Equipment
TEID	Tunnel End-point Identifier
UDP	User Datagram Protocol

3.3 Symbols

For the purposes of the present document, the following symbols apply:

Gb	Interface between an SGSN and a BSC.
Gi	Reference point between Packet Domain and an external packet data network.
Gn	Interface between two GSNs within the same PLMN.
Gp	Interface between two GSNs in different PLMNs. The Gp interface allows support of Packet Domain network services across areas served by the co-operating PLMNs.
Gs	Interface between an SGSN and MSC.
Iu	Interface between the RNS and the core network. It is also considered as a reference point.
R	The reference point between a non-ISDN compatible TE and MT. Typically this reference point supports a standard serial interface.
Um	The interface between the MS and the GSM fixed network part. The Um interface is the GSM network interface for providing packet data services over the radio to the MS. The MT part of the MS is used to access the GSM services through this interface.
Uu	Interface between the mobile station (MS) and the UMTS fixed network part. The Uu interface is the UMTS network interface for providing packet data services over the radio to the MS. The MT part of the MS is used to access the UMTS services through this interface.

4 Network characteristics

4.1 Key characteristics of PLMN

The PLMN is fully defined in the UMTS technical specifications. The Packet Domain related key characteristics are found in 3GPP TS 22.060 [2] and 3GPP TS 23.060 [3].

4.2 Key characteristics of PSDN

Void.

4.3 Key characteristics of IP Networks

The Internet is a conglomeration of networks utilising a common set of protocols. IP protocols are defined in the relevant IETF STD specifications and RFCs. The networks topologies may be based on LANs (e.g. ethernet), Point-to-Point leased lines, PSTN, ISDN, X.25 or WANs using switched technology (e.g. SMDS, ATM).

5 Interworking Classifications

5.1 Service Interworking

Service interworking is required when the Teleservice at the calling and called terminals are different. For Packet Domain, service interworking is not applicable at the Gi reference point.

5.2 Network Interworking

Network interworking is required whenever a PLMN is involved in communications with another network to provide end-to-end communications. The PLMN shall interconnect in a manner consistent with that of a normal Packet Data Network (type defined by the requirements e.g. IP). Interworking appears exactly like that of Packet Data Networks.

5.3 Numbering and Addressing

See 3GPP TS 23.003 [40] and the relevant section for IP addressing below.

6 Access reference configuration

Figure 1 shows the relationship between the MS, its terminal equipment and the UMTS/GSM network in the overall Packet Domain environment.

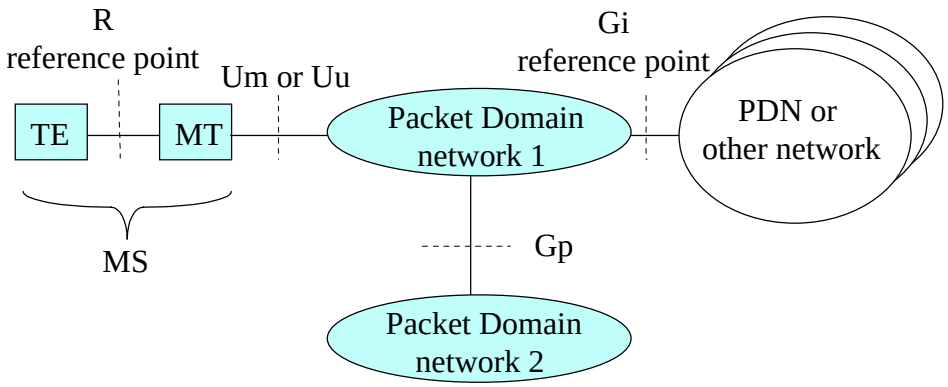


Figure 1: Packet Domain Access Interfaces and Reference Points

7 Interface to Packet Domain Bearer Services

7.1 GSM

The following figure 2a shows the relationship of the GSM Packet Domain Bearer terminating at the SNDCP layer to the rest of the GSM Packet Domain environment. It is shown for reference purposes only and detailed information can be found in 3GPP TS 23.060 [3].

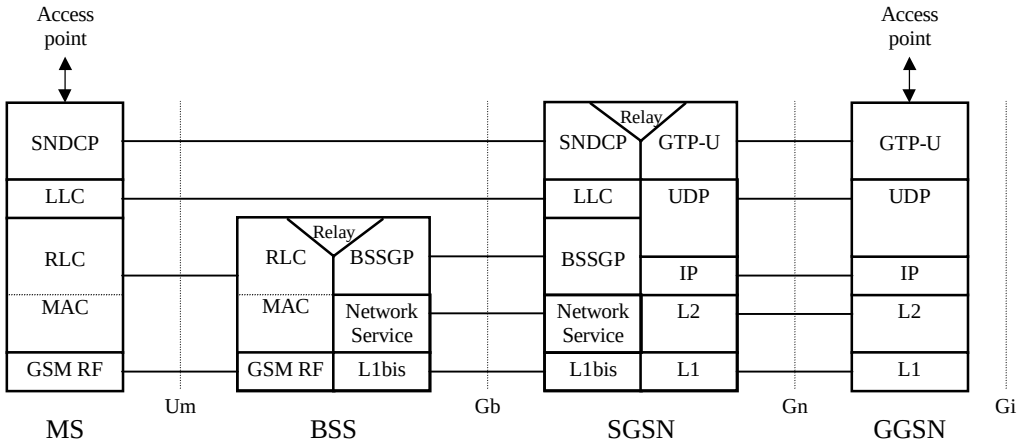


Figure 2a: User Plane for Packet Domain services in GSM

7.2 UMTS

The following figure 2b shows the relationship of the UMTS Packet Domain Bearer, terminating at the PDCP layer, to the rest of the UMTS Packet Domain environment. It is shown for reference purposes only and detailed information can be found in 3GPP TS 23.060 [3].

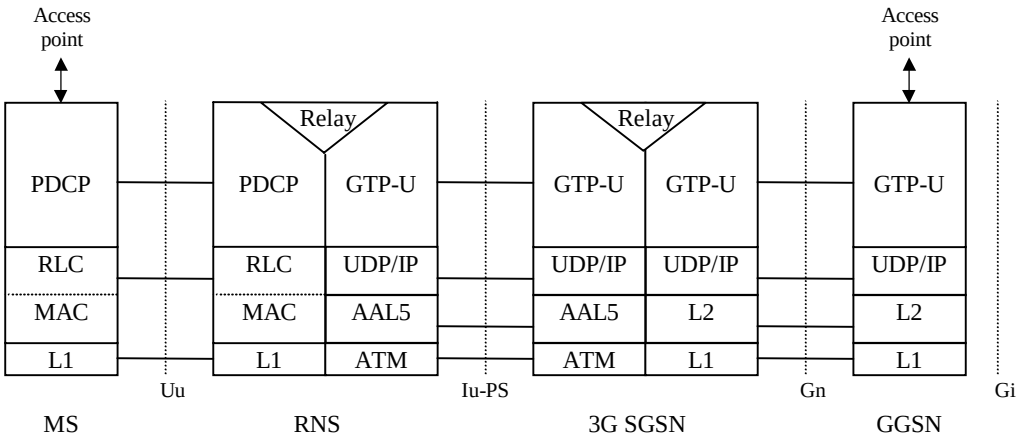


Figure 2b: User Plane for Packet Domain services in UMTS

8 Subscription checking

Subscription is checked during the PS Attach procedure and also during the PDP Context Activation procedure as described in 3GPP TS 23.060 [3]. The GGSN implicitly checks its internal context related to the destination address for each mobile terminated packet. If there is a context associated with the PDP address the packet shall be forwarded to the MS, otherwise the packet shall be discarded or rejected depending on the implemented protocol.

9 Message Screening

Screening functions reside within the Packet Domain as described in 3GPP TS 22.060 [2] and 3GPP TS 23.060 [3]. Screening may be applicable for only certain protocols. Screening is outside the scope of the present document.

10 Interworking with PSDN (X.75/X.25)

Figure 3: Void

Figure 4: Void

Figure 5: Void

Figure 6: Void

11 Interworking with PDN (IP)

11.1 General

Packet Domain shall support interworking with networks based on the Internet Protocol (IP). These interworked networks may be either intranets or the Internet.

11.2 PDN Interworking Model

When interworking with the IP networks, the Packet Domain can operate IPv4 or IPv6. The interworking point with IP networks is at the Gi reference point as shown in figure 7.

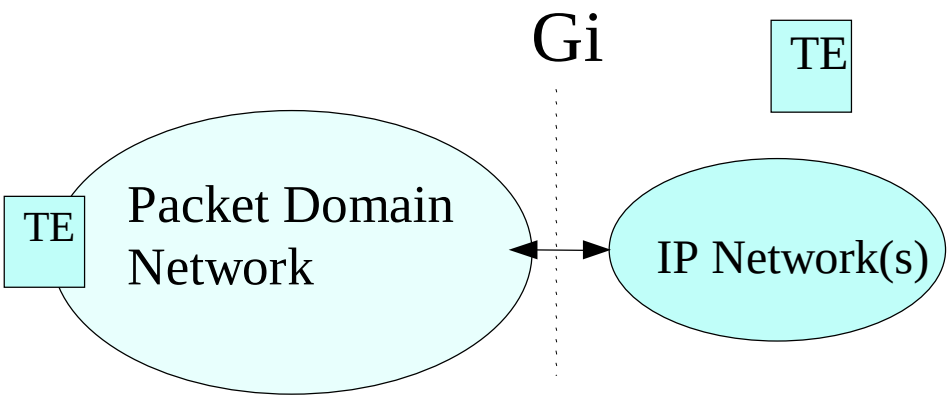


Figure 7: IP network interworking

The GGSN for interworking with the IP network is the access point of the Packet Domain (see figure 8). In this case the Packet Domain network will look like any other IP network or subnetwork.

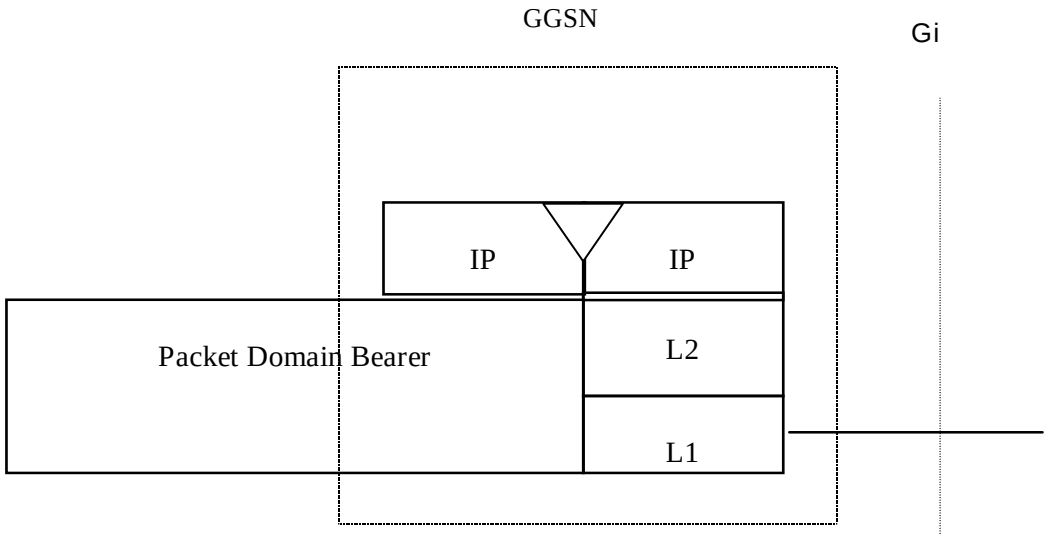


Figure 8: The protocol stacks for the IP / Gi reference point

Typically in the IP networks, the interworking with subnetworks is done via IP routers. The Gi reference point is between the GGSN and the external IP network. From the external IP network's point of view, the GGSN is seen as a normal IP router. The L2 and L1 layers are operator specific.

It is out of the scope of the present document to standardise the router functions and the used protocols in the Gi reference point.

Interworking with user defined ISPs and private/public IP networks is subject to interconnect agreements between the network operators.

No user data or header compression is done in the GGSN.

11.2.1 Access to Internet, Intranet or ISP through Packet Domain

The access to Internet, Intranet or ISP may involve specific functions such as : user authentication, user's authorization, end to end encryption between MS and Intranet/ISP, allocation of a dynamic address belonging to the PLMN/Intranet/ISP addressing space, IPv6 address autoconfiguration, etc.

For this purpose the Packet Domain may offer:

- either direct transparent access to the Internet; or
- a non transparent access to the Intranet/ISP. In this case the Packet Domain, i.e. the GGSN, takes part in the functions listed above.

The mechanisms for host configuration and user authentication described in this subclause and its subclauses are only applicable to the activation of the first context activated for a specific PDP address (using the 'PDP Context Activation Procedure'). The activation of any subsequent PDP contexts for that PDP address, using the 'Secondary PDP Context Activation Procedure', as well as the use of TFTs, is described in 3GPP TS 23.060 [3].

11.2.1.1 Transparent access to the Internet

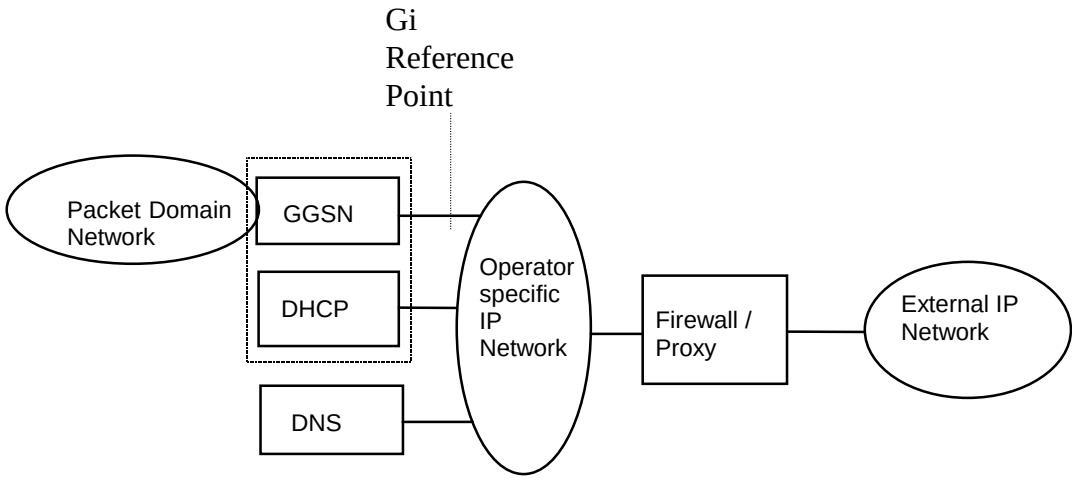


Figure 9: Example of the PDN Interworking Model, transparent case

In this case (see figure 9):

- the MS is given an address or IPv6 Prefix belonging to the operator addressing space. The address or IPv6 Prefix is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address or IPv6 Prefix is used for packet forwarding between the Internet and the GGSN and within the packet domain. With IPv6, either Stateless or Stateful Address Autoconfiguration shall be used to assign an IPv6 address to the MS. These procedures are as described in the IPv6 non-transparent access case except that the addresses belong to the operator addressing space. The use of stateful or stateless is configured per APN.

- the MS need not send any authentication request at PDP context activation and the GGSN need not take any part in the user authentication/authorization process.

The transparent case provides at least a basic ISP service. As a consequence of this it may therefore provide a bearer service for a tunnel to a private Intranet.

NB The remainder of this subclause deals with this specific case.

- The user level configuration may be carried out between the TE and the intranet, the Packet Domain network is transparent to this procedure.

The used protocol stack is depicted in figure 10.

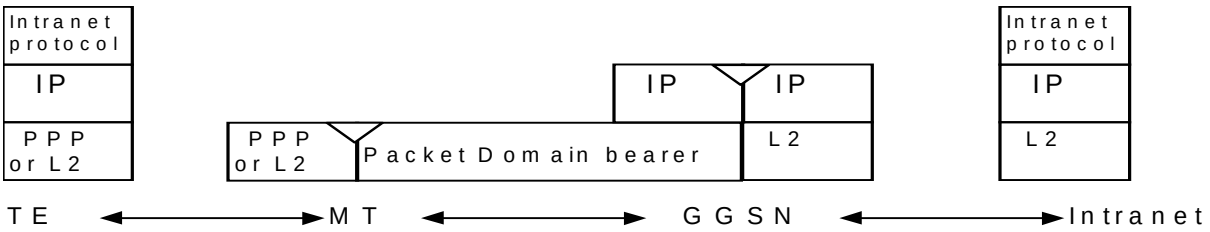


Figure 10: Transparent access to an Intranet

The communication between the PLMN and the Intranet may be performed over any network, even an insecure network e.g. the Internet. There is no specific security protocol between GGSN and the Intranet because security is ensured on an end to end basis between MS and the intranet by the "Intranet Protocol".

User authentication and encryption of user data are done within the "Intranet Protocol" if either of them is needed. This "Intranet protocol" may also carry private (IP) addresses belonging to the address space of the Intranet.

An example of an "Intranet protocol" is IPsec (see RFC 1825 [54]). If IPsec is used for this purpose then IPsec authentication header or security header may be used for user (data) authentication and for the confidentiality of user data (see RFC 1826 [55] and RFC 1827 [56]). In this case private IP tunnelling within public IP takes place.

11.2.1.2 IPv4 Non Transparent access to an Intranet or ISP

In this case:

- the MS is given an address belonging to the Intranet/ISP addressing space. The address is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address is used for packet forwarding within the GGSN and for packet forwarding on the Intranet/ISP. This requires a link between the GGSN and an address allocation server, like AAA, DHCP, …, belonging to the Intranet/ISP;

- the MS shall send an authentication request at PDP context activation and the GGSN requests user authentication from a server, like AAA, DHCP, …, belonging to the Intranet/ISP;

- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server (AAA or DHCP, …) belonging to the Intranet/ISP;

- the communication between the Packet Domain and the Intranet/ISP may be performed over any network, even an insecure e.g. the Internet. In case of an insecure connection between the GGSN and the Intranet/ISP there may be a specific security protocol in between. This security protocol is defined by mutual agreement between PLMN operator and Intranet/ISP administrator.

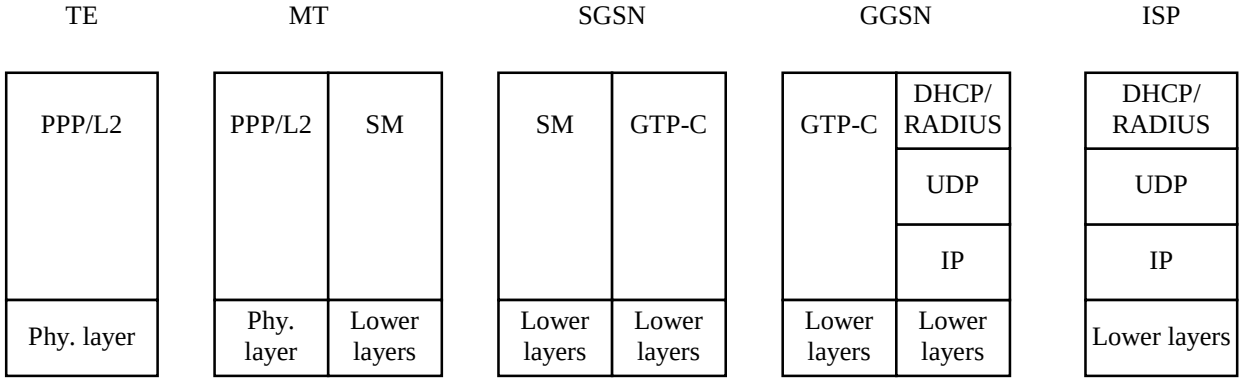


Figure 11a: Signalling plane of non transparent case

The following description bullet items describe the signal flow.

1) The TE sends an AT-command to the MT to set up parameters and enter PPP mode. The MT responds with an AT-response.

2) LCP negotiates Maximum-Receive-Unit and authentication protocol. The negotiated authentication protocol is, either CHAP, PAP or 'none'. The MT shall try to negotiate for CHAP as first priority.

3) If the negotiated authentication protocol is either of CHAP or PAP, the TE authenticates itself towards the MT by means of that protocol. The MT stores the necessary authentication data and sends a forced positive acknowledgement of the authentication to the TE.

4) The TE requests IP configuration by sending the IPCP Configure-Request message to the MT indicating either the static IP address that shall be used or that an IP-address shall be dynamically allocated.

5) The MT sends the Activate PDP context request message to the SGSN, including the Protocol Configuration Options. The SGSN sends the Create PDP context req message to the chosen GGSN including the unmodified Protocol Configuration Options.

6) The GGSN deduces from the APN:

 - the server(s) to be used for address allocation, authentication and protocol configuration options retrieval;

 - the protocol like RADIUS, DHCP, … to be used with this / those server(s);

- the communication and security feature needed to dialogue with this / those server(s) e.g. tunnel, IPSec security association, dial-up connection (using possibly PPP), …

As an example the GGSN may use one of the following options:

- RADIUS for authentication and IP-address allocation. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN;

- RADIUS for authentication and DHCP for host configuration and address allocation. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN. After a successful authentication, the DHCP client discovers the DHCP server(s) in the ISP/Intranet and receives host configuration data.

- If the received Protocol Configurations Options IE contains a PPP IPCP Configure-Request packet, the GGSN shall analyse all the contained IPCP options and their requested values. In accordance with the relevant PPP RFC 1661 [21a] and RFC 1662 [21b] the GGSN shall respond with the following messages:

 - zero or one PPP IPCP Configure-Reject packet containing options not supported and options which values cannot be returned;

 - zero or one PPP IPCP Configure-Nak packet containing options that are supported but has requested values that are incorrect/unsupported; and

 - zero or one PPP IPCP Configure-Ack packet containing options that are supported and has requested values that are correct/supported.

 Any returned PPP IPCP packets shall be contained in the Protocol Configurations Options IE.

7) The GGSN sends back to the SGSN a Create PDP Context Response message, containing the Protocol Configuration Options IE. The cause value shall be set according to the outcome of the host -authentication and -configuration. A PDP context activation shall not be rejected solely due to the presence of unsupported or incorrect PPP IPCP options or option values, received from the MS in the Protocol Configurations Options IE. The MS may however later decide to immediately deactivate the activated PDP context due to the information received in the Protocol Configurations Options IE received from the network.

8) Depending on the cause value received in the Create PDP Context Response the SGSN sends either an Activate PDP Context Accept or an Activate PDP Context Reject, to the MS.

 If Protocol Configuration Options are received from the GGSN, the SGSN shall relay those to the MS. The MT sends either the configuration-ack packet (e.g. IPCP Configure Ack in PPP case), the configure-nack packet in case of dynamic address allocation (e.g. IPCP Configure Nack in PPP case), or a link Terminate request (LCP Terminate-Request in PPP case) back to the TE. In the case where a configure-nack packet was sent by the MT, a local negotiation may take place at the R reference point (i.e. the TE proposes the new value to the MT), after which a configuration-ack packet is sent to the TE.

9) In case a configuration-ack packet was sent to the TE, the link from the TE to the external ISP/Intranet is established and IP packets may be exchanged.

 In case a link terminate request packet was sent to the TE, the TE and MT negotiates for link termination. The MT may then send a final AT-response to inform the TE about the rejected PDP Context activation.

A link terminate request packet (such as LCP Terminate-request in PPP case) causes a PDP context deactivation.

EXAMPLE: In the following example PPP is used as layer 2 protocol over the R reference point.

The MT acts as a PPP server and translates Protocol Configuration Options into SM message IEs. GTP-C carries this information unchanged to the GGSN which uses the information e.g. for DHCP or RADIUS authentication and host configuration. The result of the host authentication and configuration is carried via GTP-C to the SGSN which relays the information to the MT. The MT sends an IPCP Configure-Ack to the TE with the appropriate options included.

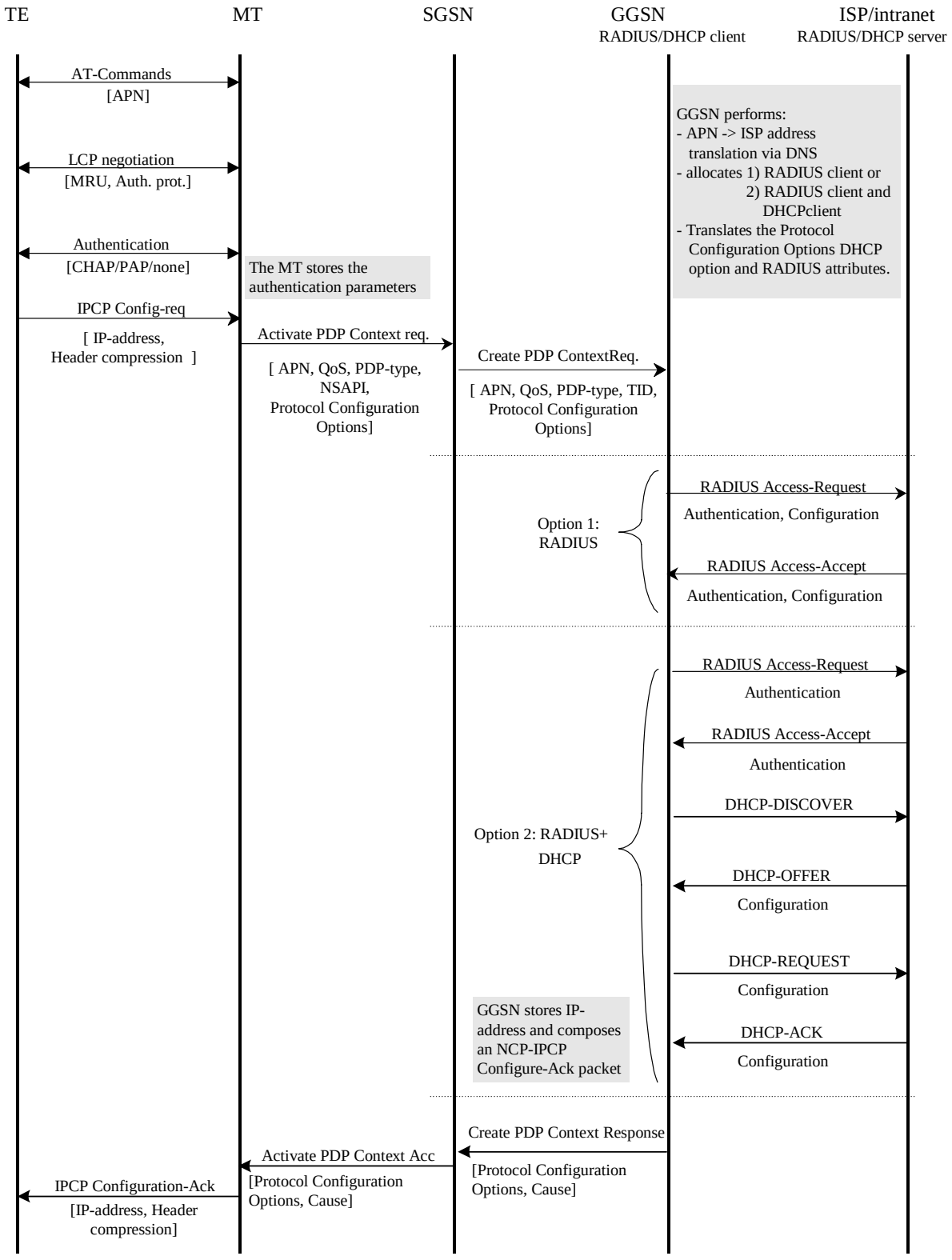


Figure 11b: PDP Context Activation for the IPv4 Non-transparent case

11.2.1.3 IPv6 Non Transparent access to an Intranet or ISP

When using IPv6 Address Autoconfiguration (either Stateless or Stateful), the process of setting up the access to an Intranet or ISP involves two signalling phases. The first signalling phase is done in the control plane and consists of the PDP context activation, followed by a second signalling phase done in the user plane.

The user plane signalling phase shall be either stateless or stateful. The stateless procedure, which involves only the MS and the GGSN, is described in subclause "IPv6 Stateless Address Autoconfiguration". The stateful procedure, which involves the MS, GGSN (as DHCP relay agent) and one or several DHCP servers on the Intranet or ISP, is described in subclause "IPv6 Stateful Address Autoconfiguration".

Whether to use stateless or stateful address autoconfiguration procedure is configured per APN in the GGSN. For APNs configured as stateless, the GGSN shall only use the Prefix part of the IPv6 address for forwarding of mobile terminated IP packets. The size of the prefix shall be according to the maximum prefix length for a global IPv6 address as specified in the IPv6 Addressing Architecture, see RFC 2373 [28].

Stateful and Stateless Autoconfiguration may also co-exist. In that case, the MS shall use Stateless to configure the address and Stateful to configure additional parameters only. The MS shall not use Stateless and Stateful Address Autoconfiguration simultaneously since GPRS only supports one prefix per PDP Context (see 3GPP TS 23.060 [3]).

The selection between Stateful and Stateless Autoconfiguration is dictated by the Router Advertisements sent by the GGSN as described in the corresponding subclauses below and according to the principles defined in RFC 2461 [44] and RFC 2462 [29].

For MS, IPv6 Stateless Address Autoconfiguration is mandatory, and IPv6 Stateful Address Autoconfiguration is optional.

11.2.1.3.1 IPv6 PDP Context Activation

In this case:

- The GGSN provides the MS with an IPv6 Prefix belonging to the Intranet/ISP addressing space. A dynamic IPv6 address shall be given using either stateless or stateful address autoconfiguration. This IPv6 address is used for packet forwarding within the packet domain and for packet forwarding on the Intranet/ISP;

- the MS may send an authentication request at PDP context activation and the GGSN may request user authentication from a server, e.g. AAA, …, belonging to the Intranet/ISP;

- the protocol configuration options are retrieved (if requested by the MS at PDP context activation) from some server, e.g. AAA, …, belonging to the Intranet/ISP;

- in order to avoid any conflict between the link-local address of the MS and that of the GGSN, the Interface-Identifier used by the MS to build its link-local address shall be assigned by the GGSN. The GGSN ensures the uniqueness of this interface-identifier. The MT shall then enforce the use of this Interface-Identifier by the TE. This is valid for both stateless and stateful address autoconfiguration.

- the communication between the Packet Domain and the Intranet/ISP may be performed over any network, even an insecure e.g. the Internet. In case of an insecure connection between the GGSN and the Intranet/ISP there may be a specific security protocol over the insecure connection. This security protocol is defined by mutual agreement between PLMN operator and Intranet/ISP administrator.

- the MS may request DNS server IPv6 addresses using the PCO IE in e.g. the PDP Context Request message. In that case the GGSN may return the IP address of one or more DNS servers in the PCO in the PDP Context Response message. The DNS address(es) shall be coded in the PCO as specified in 3GPP TS 24.008 [58]. If a list of servers is received, the MS shall adhere to the explicit prioritisation order of the list.

In the following signalling flow example, PPP is used as layer 2 protocol over the R reference point. The MT behaves as a PPP server and translates Protocol Configuration Options into SM message IEs. GTP-C carries this information unchanged to the GGSN which uses the information e.g. for RADIUS authentication. The result of the host authentication is carried via GTP-C back to the SGSN, which then relays the result to the MT. The MT finalises the IPV6CP negotiation by sending an IPV6CP Configure-Ack message to the TE with the appropriate options included, e.g. Interface-Identifier. The Interface-Identifier shall be used in the TE to create a link-local address to be able to perform the IPv6 address autoconfiguration (see subclauses 11.2.1.3.2 and 11.2.1.3.3).

1) The TE sends an AT-command to the MT to set up parameters and enter PPP mode. The MT responds with an AT-response.

2) LCP negotiates Maximum-Receive-Unit and authentication protocol. The negotiated authentication protocol is either CHAP, PAP or 'none'. The MT shall try to negotiate for CHAP as first priority.

3) If the negotiated authentication protocol is either of CHAP or PAP, the TE authenticates itself towards the MT by means of that protocol. The MT stores the necessary authentication data and sends a forced positive acknowledgement of the authentication to the TE.

4) The TE requests IPv6 Interface-Identifier negotiation by sending the IPV6CP Configure-Request message to the MT.

5) The MT sends the Activate PDP Context Request message to the SGSN, including the Protocol Configuration Options. The Protocol Configuration Options IE may contain negotiated LCP options such as negotiated Authentication Protocol as well as any authentication data previously stored in the MT. It may also contain a request for dynamic configuration of DNS server IPv6 addresses. The MS shall for dynamic address allocation leave PDP Address empty and set PDP Type to IPv6. The SGSN sends the Create PDP context request message to the chosen GGSN including the unmodified Protocol Configuration Options.

6) The GGSN deduces from local configuration data associated with the APN:

 - IPv6 address allocation type (stateless or stateful);

 - the source of IPv6 Prefixes in the stateless case (GGSN internal prefix pool, or external address allocation server);

 - any server(s) to be used for address allocation, authentication and/or protocol configuration options retrieval (e.g. IMS related configuration, see 3GPP TS 24.229 [47]);

 - the protocol e.g. RADIUS, to be used with the server(s);

 - the communication and security feature needed to communicate with the server(s);

 As an example the GGSN may use one of the following options:

 - GGSN internal Prefix pool for IPv6 prefix allocation and no authentication;

 - GGSN internal Prefix pool for IPv6 prefix allocation and RADIUS for authentication. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN;

 - RADIUS for authentication and IPv6 prefix allocation. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN;

NOTE: DHCPv6 may be used for IPv6 prefix allocation.

 IPv6 Prefixes in a GGSN internal Prefix pool shall be configurable and structured per APN.

 The GGSN shall in the PDP Address IE in the Create PDP Context Response return an IPv6 address composed of a Prefix and an Interface-Identifier. The Interface-Identifier may have any value and it does not need to be unique within or across APNs. It shall however not conflict with the Interface-Identifier the GGSN has selected for its own side of the MS-GGSN link. The Prefix assigned by the GGSN or the external AAA server shall be globally or site-local unique, if stateless address autoconfiguration is configured on this APN. If, on the other hand, stateful address autoconfiguration is configured on the APN, the Prefix part of the IPv6 address returned in the PDP Address IE shall be set to the link-local prefix (FE80::/64).

 The GGSN shall analyse the requested values of all the protocol options contained in the received Protocol Configurations Options IE. The GGSN response shall be in accordance with the relevant standards e.g. the PPP standards RFC 1661 [21a] and RFC 1662 [21b].

7) The GGSN sends back to the SGSN a Create PDP Context Response message, containing the PDP Address IE and the Protocol Configuration Options IE. The Protocol Configuration Options IE may contain configuration data such as a list of DNS server IPv6 addresses. The cause value shall be set according to the outcome of the host authentication and configuration.

8) Depending on the cause value received in the Create PDP Context Response, the SGSN either stores the PDP Address and sends an Activate PDP Context Accept to the MS or, sends an Activate PDP Context Reject, to the MS.

 If Protocol Configuration Options are received from the GGSN, the SGSN shall relay those to the MS.

9) The MT extracts the Interface-Identifier from the address received in the PDP Address IE and ignores the Prefix part. If this Interface-Identifier is identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE, the MT sends an IPV6CP Configure Ack packet, indicating this Interface-Identifier, to the TE.

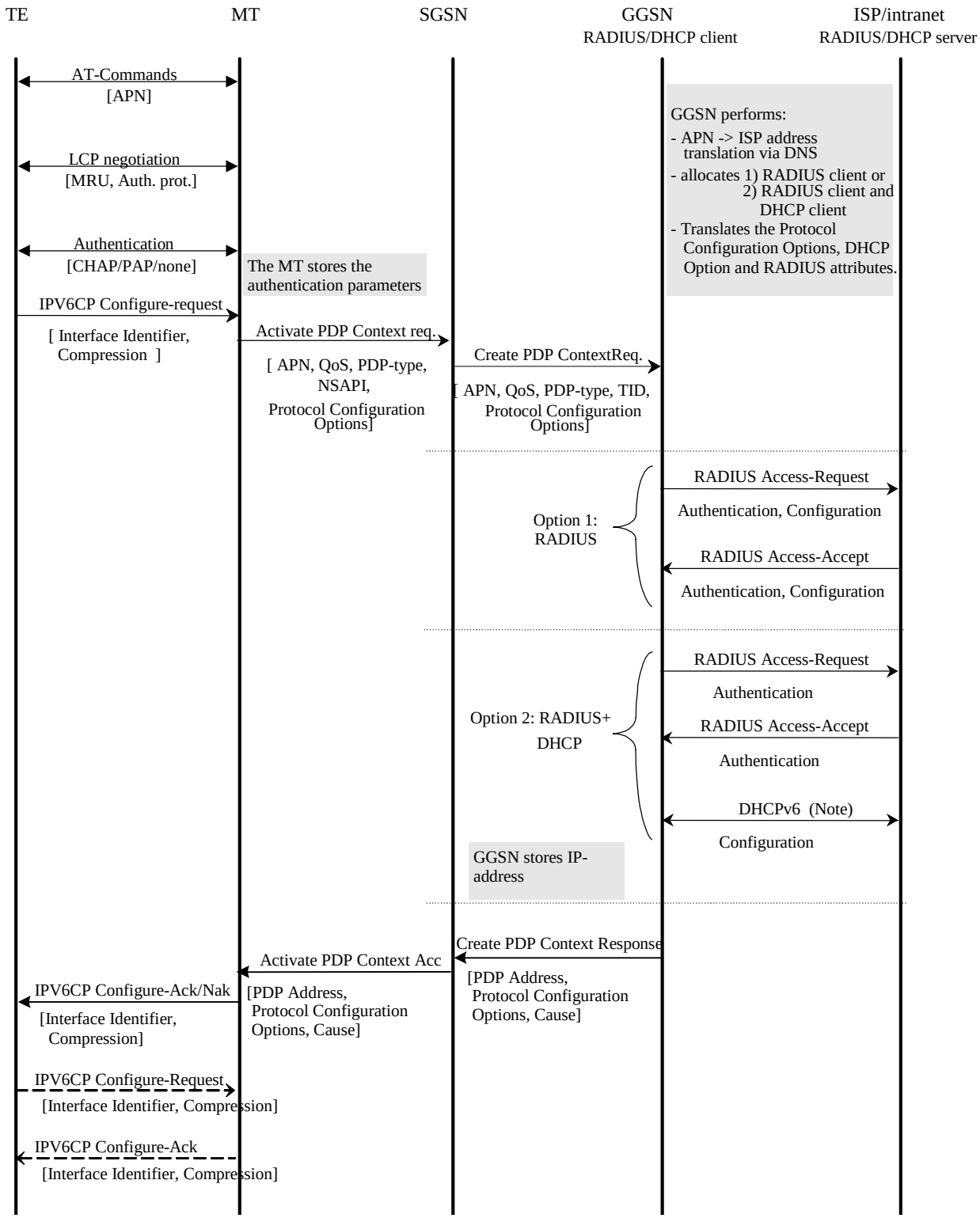
 If the Interface-Identifier extracted from the address contained in the PDP Address IE is not identical to the tentative Interface-Identifier indicated in the IPV6CP Configure-Request message sent from the TE, the MT sends an IPV6CP Configure-Nak packet, indicating the Interface-Identifier extracted from the address contained in the PDP Address IE, to the TE. The TE then sends a new IPV6CP Configure-Request message to the MT, indicating the same Interface-Identifier as was indicated in the received IPV6CP Configure Nak (as indicated by the dotted IPV6CP Configure-Request and Configure-Ack in the figure below). Finally the MT responds with a IPV6CP Configure Ack packet.

 In case a PDP Context Reject was sent to the MS the MT sends an LCP Terminate-Request to the TE.

10) When the TE has accepted the Interface-Identifier given by the MT, the user plane link from the TE to the GGSN and the external ISP/Intranet is established and the IPv6 address autoconfiguration may proceed.

 In case a link terminate request packet was sent to the TE, the TE and MT negotiates for link termination. The MT may then send a final AT-response to inform the TE about the rejected PDP Context activation.

 An LCP Terminate-request causes a PDP context deactivation.



NOTE: DHCPv6 may be used for IPv6 prefix allocation.

Figure 11ba: PDP Context Activation for the IPv6 Non-transparent case

Figure 11ba is valid for both Stateless and Stateful Address Autoconfiguration case. In the Stateful case though, option 2 does not apply and option 1 may only be used for authentication. The use of DHCPv6 above is different and used in a different context than when used for Stateful Address Autoconfiguration as in subclause 11.2.1.3.3.

11.2.1.3.2 IPv6 Stateless Address Autoconfiguration

As described in 3GPP TS 23.060 [3], a PDP Context of PDP type IPv6 activated by means of the IPv6 Stateless Address Autoconfiguration Procedure is uniquely identified by the prefix part of the IPv6 address only. The MS may select any value for the Interface-Identifier part of the address. The only exception is the Interface-Identifier for the link-local address used by the MS (see RFC 2373 [28]). This Interface-Identifier shall be assigned by the GGSN to avoid any conflict between the link-local address of the MS and that of the GGSN itself. This is described in subclause "IPv6 PDP Context Activation" above.

For IPv6 the PDP Context Activation phase is followed by an address autoconfiguration phase. The procedure describing APNs configured to use Stateless Address Autoconfiguration, may be as follows:

1) After the first phase of setting up IPv6 access to an Intranet or ISP, the MS shall use the IPv6 Interface-Identifier, as provided by the GGSN, to create its IPv6 Link-Local Unicast Address according to RFC 2373 [28].

 Before the MS can communicate with other hosts or MSes on the Intranet/ISP, the MS must obtain an IPv6 Global or Site-Local Unicast Address. The simplest way is the IPv6 Stateless Address Autoconfiguration procedure described below and in 3GPP TS 23.060 [3]. The procedure is consistent with RFC 2462 [29].

 The procedure below takes place through signalling in the user plane. It is done on the link between the MS and the GGSN. From the MS perspective the GGSN is now the first router on the link.

2) After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately.

 To indicate to the MS that stateless address autoconfiguration shall be performed, the GGSN shall leave the M-flag cleared in the Router Advertisement messages. An MS shall not perform stateless and stateful address autoconfiguration simultaneously, since multiple prefixes are not allowed in GPRS. The O-flag may be set though, since it does not result in additional addresses being acquired (see below).

 The Prefix sent in the Router Advertisements shall be identical to the Prefix returned in the Create PDP Context Response. The Prefix is contained in the Prefix Information Option of the Router Advertisements and shall have the A-flag set ("Autonomous address configuration flag") and the L-flag cleared (i.e. the prefix should not be used for on-link determination). The lifetime of the prefix shall be set to infinity. In practice, the lifetime of a Prefix will be the lifetime of its PDP Context. There shall be exactly one Prefix included in the Router Advertisements.

 The handling of Router Advertisements shall be consistent with what is specified in RFC 2461 [44]. For the MS-GGSN link however, some specific handling shall apply. The randomisation part to determine when Router Advertisements shall be sent may be omitted since the GGSN is the only router on the link. Furthermore, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN"). These relate to the periodicity of the Router Advertisements initially and during continued operation. The motivation for this is to have a faster user-plane set-up even in bad radio conditions and to minimize MS power consumption during long continued operation.

3) When creating a Global or Site-Local Unicast Address, the MS may use the Interface-Identifier received during the PDP Context Activation phase or it may generate a new Interface-Identifier. There is no restriction on the value of the Interface-Identifier of the Global or Site-Local Unicast Address, since the Prefix is unique. Interface-Identifiers shall in any case be 64-bit long.

 Since the GGSN guarantees that the Prefix is unique, the MS does not need to perform any Duplicate Address Detection on addresses it creates. That is, the 'DupAddrDetectTransmits' variable in the MS should have a value of zero. If the MS finds more than one Prefix in the Router Advertisement message, it shall only consider the first one and silently discard the others. The GGSN shall not generate any globally unique IPv6 addresses for itself using the Prefix assigned to the MS in the Router Advertisement.

 If the O-flag ("Other stateful configuration flag") was set in the Router Advertisement, the MS may start a DHCP session to retrieve additional configuration parameters. See subclause 13.2.2 "Other configuration by the Intranet or ISP". If the MS is not DHCP capable, the O-flag may be ignored.

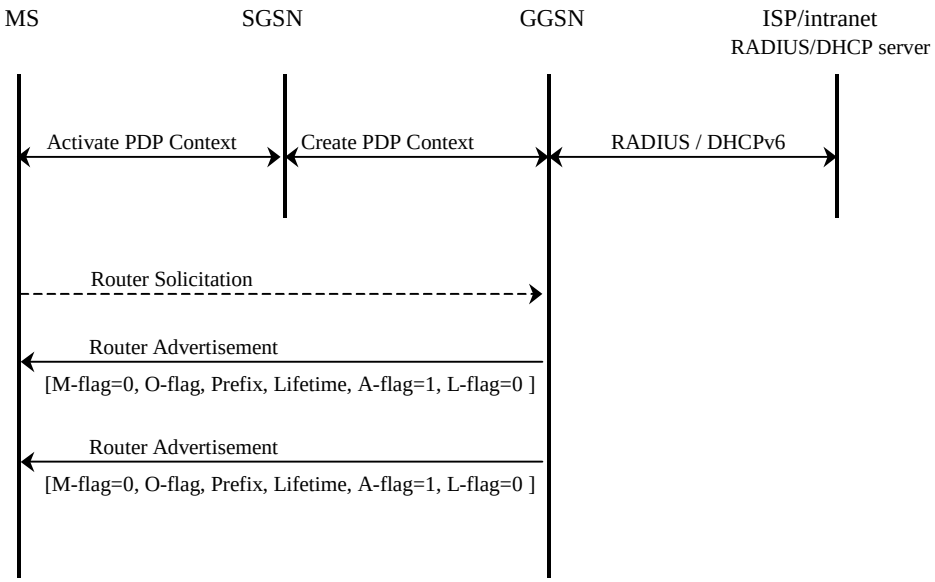


Figure 11bb: IPv6 Stateless Address Autoconfiguration

11.2.1.3.3 IPv6 Stateful Address Autoconfiguration

For IPv6 the PDP Context Activation phase is followed by an address autoconfiguration phase. For APNs configured to use Stateful Address Autoconfiguration, the procedure may for example look like below. A more detailed description of Stateful Address Autoconfiguration is described in clause "Interworking with PDN (DHCP)". Support of DHCP is not mandatory in the MS.

1) After the first phase of setting up IPv6 access to an Intranet or ISP, the MS shall use the IPv6 Interface-Identifier, as provided by the GGSN, to create its IPv6 Link-Local Unicast Address according to RFC 2373 [28].

2) After the GGSN has sent a Create PDP Context Response message to the SGSN, it shall start sending Router Advertisements periodically on the new MS-GGSN link established by the PDP Context. The MS may issue a Router Solicitation directly after the user plane establishment. This shall trigger the GGSN to send a Router Advertisement immediately. This shall be consistent with what is specified in RFC 2461 [44]. For the MS-GGSN link however, some 3GPP specific protocol constants and default values shall apply (see subclause "IPv6 Router Configuration Variables in the GGSN").

 To indicate to the MS that Stateful Address Autoconfiguration shall be performed, the Router Advertisements shall not contain any Prefix-Information option and the M-flag ("Managed Address Configuration Flag") shall be set.

3) When the MS has received a Router Advertisement with the M-flag set, it shall start a DHCPv6 configuration as described in subclause "Address allocation using DHCPv6" including a request for an IPv6 address.

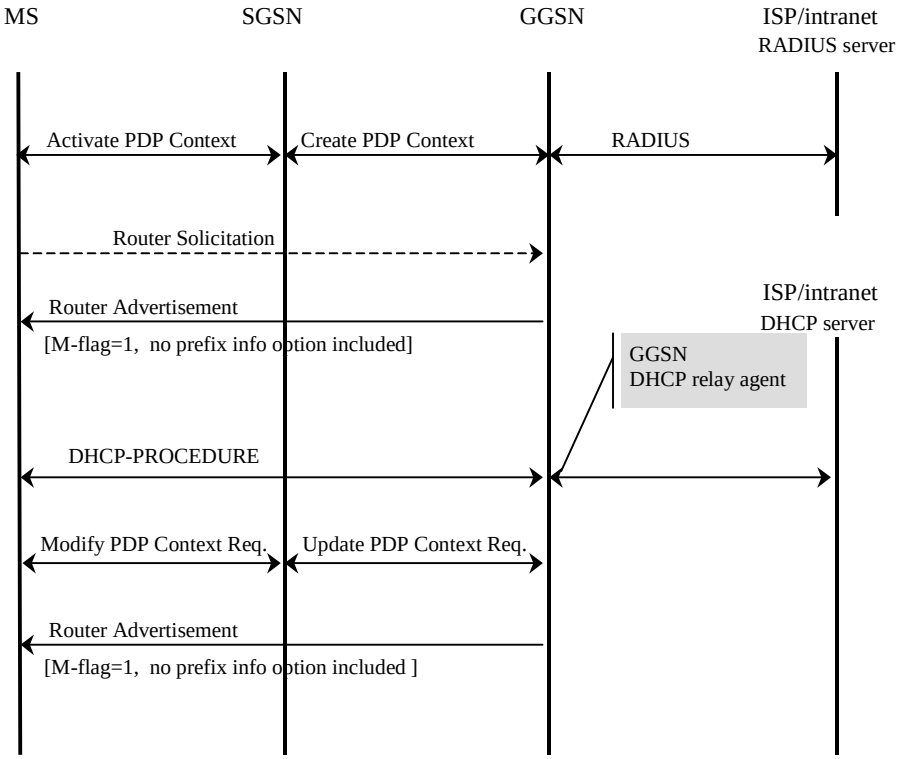


Figure 11bc: IPv6 Stateful Address Autoconfiguration

11.2.1.3.4 IPv6 Router Configuration Variables in the GGSN

For IPv6 Stateless and Stateful Address Autoconfiguration to work properly the GGSN shall behave as an IPv6 router towards the MS. In this respect the GGSN shall be consistent with the RFCs specifying this process (for example RFC 2462 [29] and RFC 2461 [44]), unless stated otherwise in this or other 3GPP specifications.

RFC 2461 [44] specifies a set of conceptual router configuration variables. Some of these variables require particular attention in GPRS in order to preserve radio resources and MS power consumption while still allowing for appropriate robustness and fast user-plane set-up time even in bad radio conditions, or simply because they have a particular meaning in GPRS. These particular variables are listed below with appropriate (default) values and shall be configurable per APN. The values specified hereafter are specific to GPRS and supersede those specified in RFC 2461 [44].

MaxRtrAdvInterval

Shall have a default value of 21 600 seconds (6 h).

MinRtrAdvInterval

Shall have a default value of 0.75 × MaxRtrAdvInterval i.e.16 200 seconds (4.5 h).

AdvValidLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF. The assigned prefix remains Preferred until PDP Context Deactivation.

AdvPreferredLifetime

Shall have a value giving Prefixes infinite lifetime, i.e. 0xFFFFFFFF. The assigned prefix remains Preferred until PDP Context Deactivation.

RFC 2461 [44] also specifies a number of protocol constants. The following shall have specific values for GPRS:

MAX_INITIAL_RTR_ADVERT_INTERVAL

This constant may be a variable within GPRS. It may have a value that gradually increases (exponentially or by some other means) with the number of initial Router Advertisements sent. This will enable a fast set-up of the MS-GGSN link in most cases, while still allowing the MS to receive a Router Advertisement within the initial phase, even in case of bad radio conditions or slow response time, without having to send a large number of initial Router Advertisements.

MAX_INITIAL_RTR_ADVERTISEMENTS

This is the number of Router Advertisements sent during the initial phase after the MS-GGSN link has been established. The value of this constant shall be chosen carefully, and in conjunction with MAX_INITIAL_RTR_ADVERT_INTERVAL, so as to not overload the radio interface while still allowing the MS to complete its configuration in a reasonable delay. For instance, the default value could be chosen so that initial Router Advertisements are sent for at least 30 seconds.

After the initial phase, the periodicity is controlled by the MaxRtrAdvInterval and the MinRtrAdvInterval constants.

11.2.1.4 Access to Internet, Intranet or ISP with Mobile IPv4

General

A way to allow users to roam from one environment to another, between fixed and mobile, between public and private as well as between different public systems is to use Mobile IP RFC 2002 [30]. Mobile IP (MIP) is a mobility management protocol developed by IETF. The Mobile IP Foreign Agent (FA) RFC 2002 [30] is located in the Core Network in the GGSN. MIP also uses a Home Agent (HA) RFC 2002 [30] which may or may not be located in a GSM/UMTS network.

Interworking model for MIP

A FA is located in the GGSN. The interface between the GGSN and the FA will probably not be standardised as the GGSN/FA is considered being one integrated node. The mapping between these two is a matter of implementation. Each FA must be configured with at least one care-of address. In addition a FA must maintain a list that combines IP addresses with TEIDs of all the visiting MSs that have registered with the FA. IP packets destined for the MS are intercepted by the HA and tunneled to the MS's care-of address, i.e. the FA. The FA de-tunnels the packets and forwards the packets to the MS. Mobile IP related signalling between the MS and the FA is done in the user plane. MIP registration messages RFC 2002 [30] are sent with UDP.

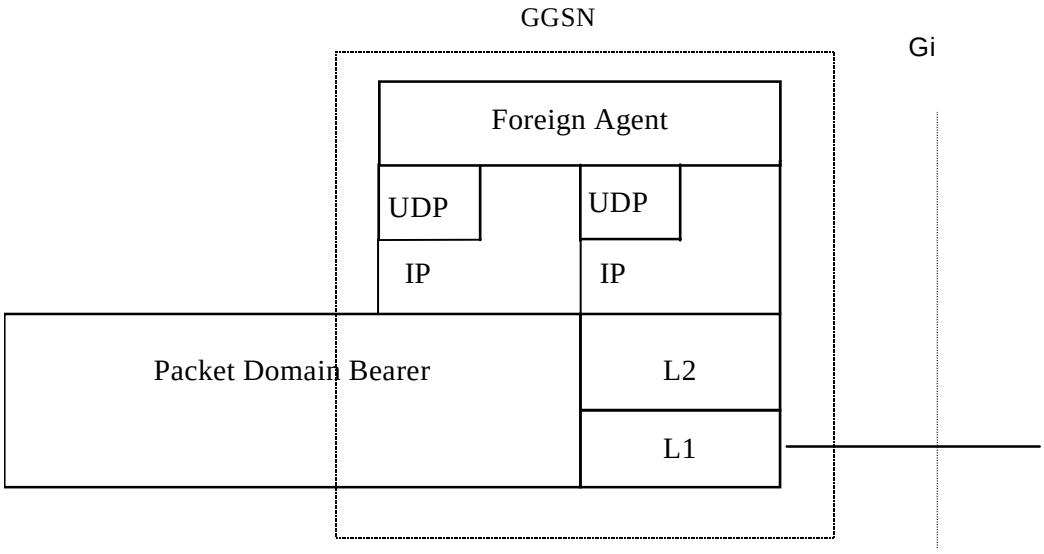


Figure 11c: The protocol stacks for the Gi IP reference point in the MIP signalling plane

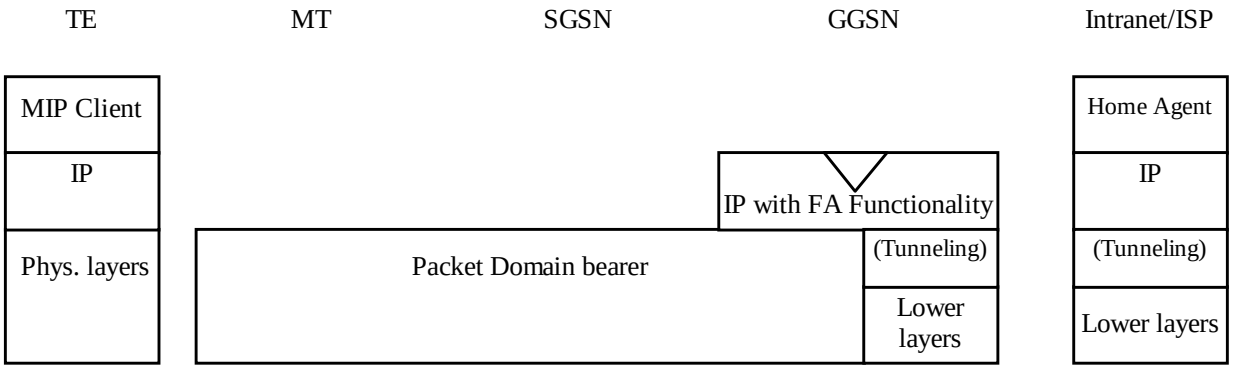


Figure 11d: Protocol stacks for user access with MIP

In figure 11d: "(Tunneling)" is intended to show asymmetric traffic flow. Tunneling (IP-in-IP) is only used in the direction from the ISP towards the MT.

Authentication of the user is supported in Mobile IPv4. This authentication mechanism may involve communication with an authentication server (e.g. RADIUS), although this is not shown in figure 11d.

Address allocation - at PDP context activation no IP address is allocated to the MS indicated by 0.0.0.0. in the "Requested PDP Address" field. If the MS does not have a static IP address which it could register with the HA, it will acquire a dynamic IP address from the HA RFC 2794 [25]. After completion of the PDP activation the SGSN is informed of the assigned IP address by means of the GGSN initiated PDP Context Modification Procedure.

An example of a signalling scheme, shown in figure 11e, is described below. In this example the MS is separated into a TE and MT, with AT commands and PPP used in-between (see 3GPP TS 27.060 [10]). The PS attach procedures have been omitted for clarity.

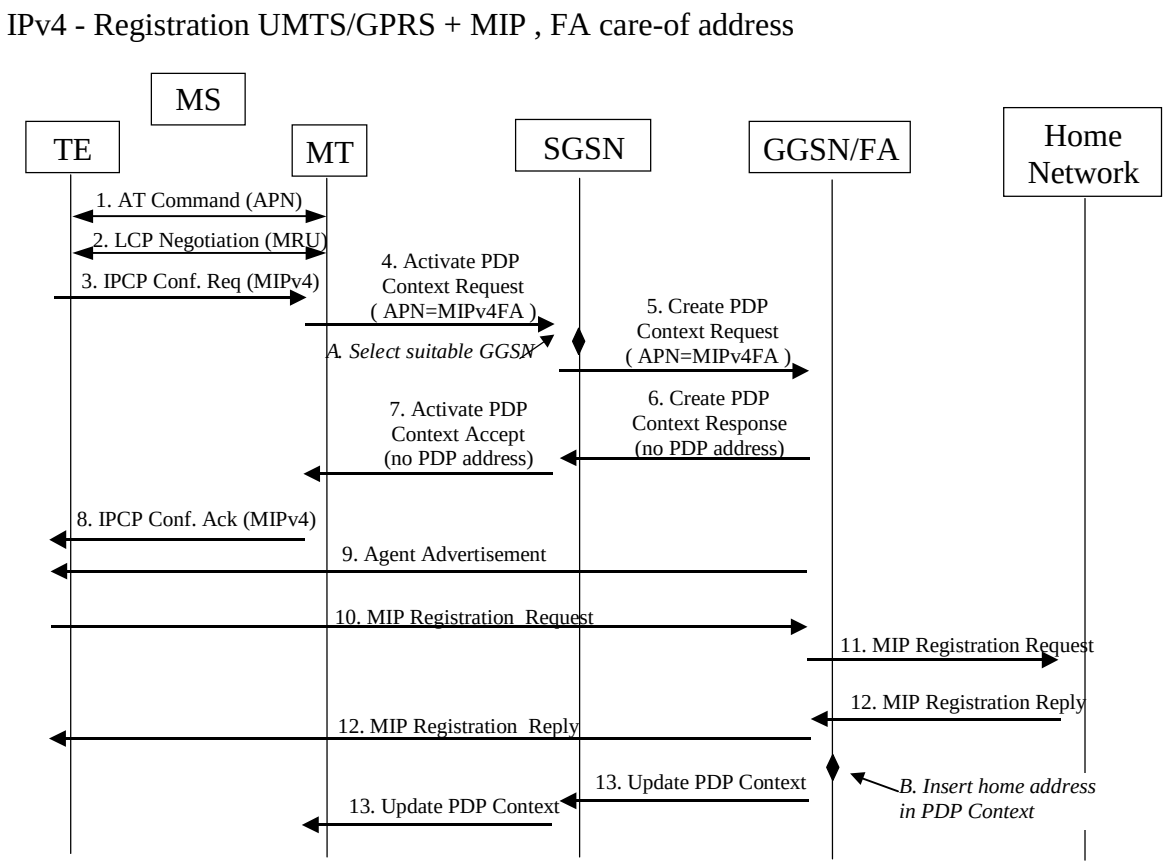


Figure 11e: Example of PDP Context activation with Mobile IP registration (the PS attach procedure not included)

1. The AT command carries parameters that the MT needs to request the PDP Context Activation. The important parameter here, is the APN (Access Point Name), see clause A below. The AT command is followed by a setup of the PPP connection between the MT and the TE.

2. As part of the PPP connection, LCP negotiates Maximum-Receive-Unit between the TE and the MT. No PPP authentication is required when using MIPv4.

3. As part of the PPP connection, the TE sends an IPCP Configure Request using the MIPv4 configuration option (see RFC 2290 [37]). The TE sends either its Home Address or a null address (i.e. 0.0.0.0) if the Network Address identifier is used (see RFC 2794 [25]).

4. The MT sends the "Activate PDP Context Request" to the SGSN. The message includes various parameters of which the "APN" (Access Point Name) and the "Requested PDP Address" are of interest here. The TE/MT may use APN to select a reference point to a certain external network or to select a service. APN is a logical name referring to the external packet data network or to a service that the subscriber wishes to connect to. The "Requested PDP Address" should be omitted for all MSs using Mobile IP. This is done irrespective of if the TE has a permanently assigned Mobile IP address from its Mobile IP home network, a previously assigned dynamic home address from its Mobile IP home network or if it wishes the Mobile IP home network to allocate a "new" dynamic home address.

 A. The SGSN will base the choice of GGSN based on the APN that is given by the MS.

5. The SGSN requests the selected GGSN to set up a PDP Context for the MS. The PDP address and APN fields are the same as in the "Activate PDP Context Request" message.

6. A Create PDP Context Response is sent from the GGSN/FA to the SGSN. If the creation of PDP Context was successful, some parameters will be returned to the SGSN, if not, an error code will be returned. If the GGSN has been configured, by the operator, to use a Foreign Agent for the requested APN, the PDP address returned by the GGSN shall be set to 0.0.0.0. indicating that the PDP address shall be reset by the MS with a Home Agent after the PDP context activation procedure.

7. The Activate PDP Context Accept message is sent by the SGSN to the MT and contains similar information as the Create PDP Context Response message.

8. The MT sends an IPCP Configure Ack to the TE in order to terminate the PPP connection phase.

9. The Agent Advertisement RFC 2002 [30] is an ICMP (Internet Control Message Protocol) Router Advertisement message with a mobility agent advertisement extension. The latter part contains parameters of the FA that the mobile node needs, among those are one or more care-of addresses that the FA offers. This message should be sent, in the Packet Domain user plane, as an IP limited broadcast message, i.e. destination address 255.255.255.255, however only on the TEID for the requesting MS to avoid broadcast over the radio interface.

10. The Mobile IP Registration Request is sent from the mobile node to the GGSN/FA across the Packet Domain backbone as user traffic. The mobile node includes its (permanent) home address as a parameter RFC 2002 [30]. Alternatively, it can request a temporary address assigned by the home network by sending 0.0.0.0 as its home address, and include the Network Access Identifier (NAI) in a Mobile-Node-NAI Extension RFC 2794 [25], RFC 2486 [31].

11. The FA forwards the Mobile IP Registration Request to the home network of the mobile node, where a home agent (HA) processes it. Meanwhile, the GGSN/FA needs to store the home address of the mobile node or the NAI and the local link address of the MS, i.e. the TEID (Tunnel Endpoint ID).

12. The Registration Reply is sent from the home network to the FA, which extracts the information it needs and forwards the message to the mobile node in the Packet Domain user plane. As the FA/GGSN knows the TEID and the NAI or home address, it can pass it on to the correct MS.

 B. The GGSN/FA extracts the home address from the Mobile IP Registration Reply message and updates its GGSN PDP Context.

13. The GGSN triggers a "GGSN initiated PDP Context modification procedure" in order to update the PDP address in the SGSN and in the MT.

11.3 Numbering and Addressing

In the case of interworking with public IP networks (such as the Internet), the PLMN operator shall use public network addresses. These public addresses can be reserved from the responsible IP numbering body, or from an ISP with which the PLMN operator has an agreement. In case of IPv6, a global IPv6 prefix can be obtained from the same sources.

In the case of interworking with private IP networks, two scenarios can be identified:

1. the GPRS operator manages internally the subnetwork addresses or IPv6 prefixes. Each private network is assigned a unique subnetwork address or range of IPv6 prefixes. Normal routing functions are used to route packets to the appropriate private network;

2. each private network manages its own addressing. In general this will result in different private networks having overlapping address ranges. A logically separate connection (e.g. an IP in IP tunnel or layer 2 virtual circuit) is used between the GGSN and each private network. In this case the IP address alone is not necessarily unique. The pair of values, Access Point Name (APN) and IP address or IPv6 prefix, is unique.

NOTE: In IPv6 "site-local addresses" replace "private addresses" in IPv4, see RFC 2373 [28]. Site-local addresses may be used when a site (e.g. a corporate network) requires local administration of its address space.

The PLMN operator allocates the IP addresses for the subscribers in either of the following ways.

- The PLMN operator allocates a static IP address (IPv4 or IPv6) when the subscription record is built. The IP address is reserved from a pool of free IP addresses. Each external network has its own pool of addresses.

- The PLMN operator allocates (either on its own or in conjunction with the external network) a dynamic IP (IPv4 or IPv6) address or IPv6 prefix as described in 3GPP TS 23.060 [3].

11.4 Charging

The PLMN operator may define the accuracy of the charging mechanism using one of the following categories:

- every source/destination pair is logged separately;

- source/destination pairs are logged to an accuracy of subnetworks;

- source/destination pairs are logged to an accuracy of connection types (e.g. external data network, corporate network, another mobile).

11.5 Domain Name System Server (DNS Server)

Provision of Domain Name services shall be provided by the PLMN operators in the transparent case and the ISP in the non transparent case. (DNS documentation is provided in RFC 1034 [19] and RFC 1035 [52]).

11.6 Screening

The way the PLMN is performing the operator controlled screening and the subscription controlled screening is out of the scope of the present document. These functions may be done, for example, in a firewall.

11.7 IP Multicast access

The Packet Domain could allow access to IP Multicast traffic coming from an external network. The support of IP-Multicast in the Packet Domain is optional.

In order for the Packet Core Network to support Multicast traffic that will allow the MS to subscribe to multicast groups from outside the PLMN, the GGSN shall support IGMP (IPv4) and/or MLD (IPv6) and one or more Inter-Router Multicast protocols, such as DVMRP, MOSPF, or PIM-SM.

IGMP/MLD is an integral part of IP. All hosts wishing to receive IP multicasts are required to implement IGMP (or equivalent) and class-D IPv4 addresses of MLD and IPv6 multicast according to RFC 2710 [48]. IGMP/MLD messages are encapsulated in IP datagrams.

To be able to deliver IP-Multicast packets to the appropriate TEs, the GGSN may have an IP-Multicast proxy functionality.

The IP-Multicast proxy will perform the following tasks:

NOTE: In this example it is assumed that IGMP/MLD is used as a Host-Router Multicast protocol.

- maintain a list of mobiles that joined one or more Multicast groups. This list is built/updated each time the GGSN receives an IGMP Join or MLD Report message from the mobile;
- send, based on this maintained list of mobiles, multicast routing information to the routers attached to the Packet Domain, allowing them to route multicast packets;
- upon reception by the GGSN of multicast packets, make and send a copy as Point-to-Point packets, to each mobile of the group.

IP-Multicast traffic can only be handled after an MS has attached to the Packet Domain, and Activated PDP context(s) (including possibly authentication) to the preferred ISP/external network. The Multicast traffic is handled at the application level from a Packet Domain perspective and is sent over UDP/IP.

The following figure 12 depicts the protocol configuration for handling Multicast traffic (control plane). The Multicast traffic handling affects the GGSN by the introduction of the IP-Multicast proxy and the support for an Inter-Router Multicast protocol and a host-router multicast protocol.

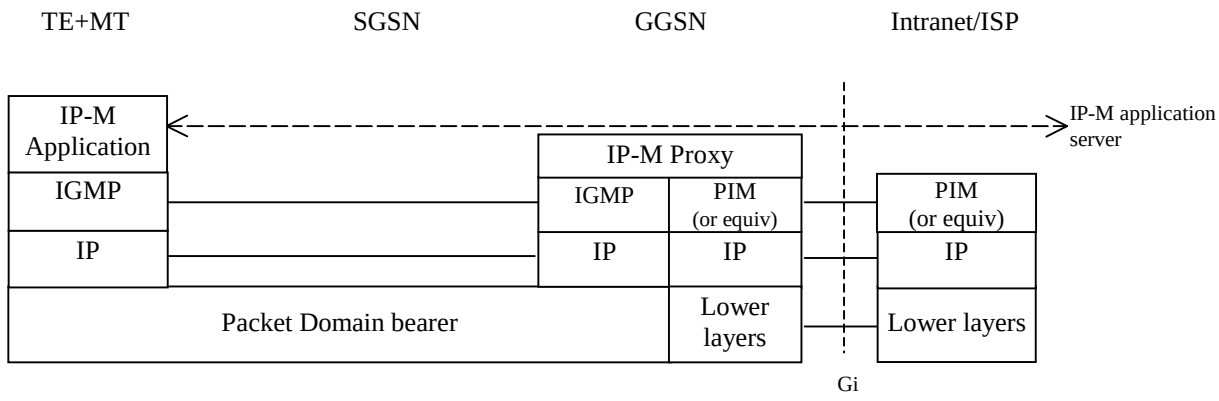


Figure 12: Protocol configuration for IP-Multicast handling (control plane)

12 Interworking with PDN (PPP)

12.1 General

By means of the PDP type 'PPP' Packet Domain may support interworking with networks based on the point-to-point protocol (PPP), as well as with networks based on any protocol supported by PPP through one of its Network Control Protocols (NCPs). All protocols currently supported by PPP NCPs are listed in RFC 1661 [21a] and RFC 1662 [21b]. It may also support interworking by means of tunnelled PPP, by e.g. the Layer Two Tunnelling Protocol (L2TP).

12.2 PDN Interworking Model

The interworking point is at the Gi reference point. The GGSN for interworking with the ISP/PDN is the access point of the Packet Domain (see figure 13). The GGSN will either terminate the PPP connection towards the MS or may further relay PPP frames to the PDN. The PPP frames may be tunnelled in e.g. L2TP.

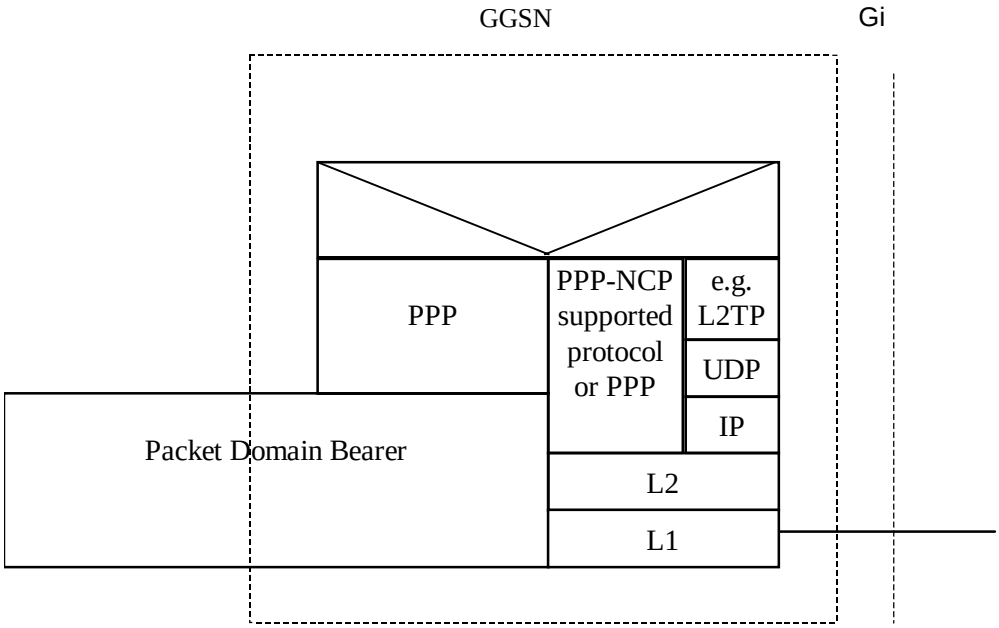


Figure 13: The protocol stacks for the Gi PPP reference point

In case the external PDN is an IP based network and the GGSN terminates PPP the same description applies as specified in subclause 11.2.

In case the GGSN tunnels PPP frames to the PDN, the GGSN may behave like a LAC towards the external network.

12.2.1 Virtual dial-up- and direct Access to PDNs, or ISPs through Packet Domain

The access to PDNs, or ISPs may involve specific functions such as: user authentication, user's authorization, end to end encryption between MS and PDN/ISP, allocation of a dynamic address belonging to the PLMN/PDN/ISP addressing space, etc.

For this purpose the PLMN may offer, based on configuration data:

- direct access to an IP based Intranet/ISP using a protocol configuration as depicted in figure 14. Here DHCP and/or RADIUS are used between the GGSN and Intranet/ISP for performing the specific functions mentioned above. The Packet Domain may also offer access to networks based on any protocol supported by PPP through one of its Network Control Protocols (NCPs);

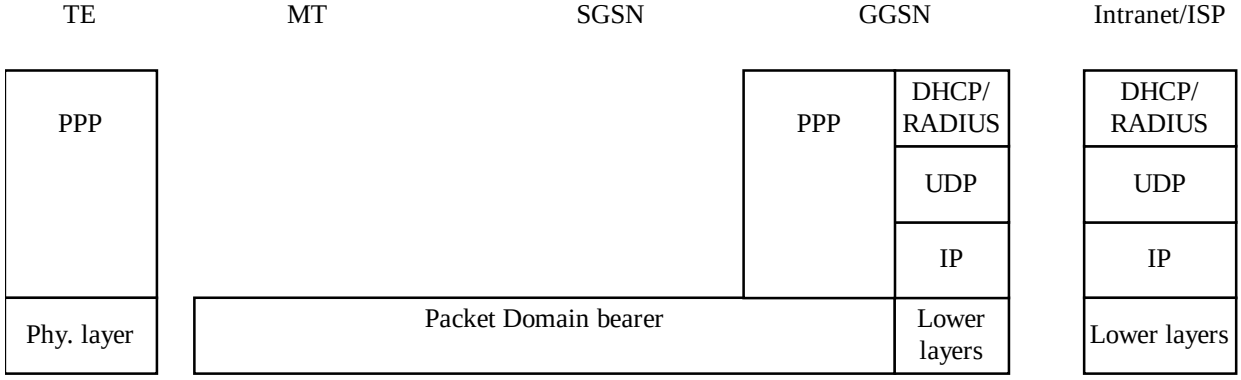


Figure 14: Protocol stack for direct access to IP-based Intranets/ISPs

- virtual dial-up access to a PDN with PPP frame tunnelling as depicted in figure 15.

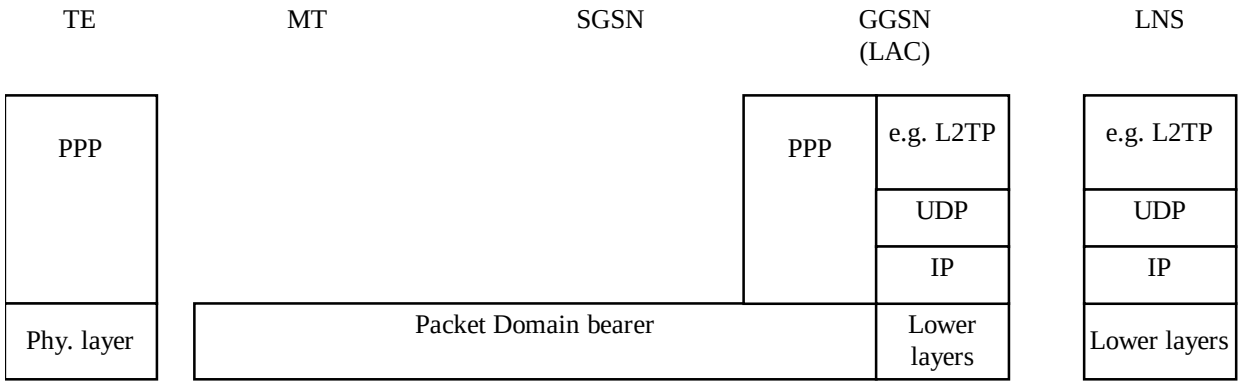


Figure 15: Protocol stack for virtual dial-up access with PPP frame tunnelling

12.2.1.1 Procedural description

In this case:

- the MS is given an address belonging to the Intranet/ISP addressing space. The address is given either at subscription in which case it is a static address or at PDP context activation in which case it is a dynamic address. This address is used for packet forwarding within the GGSN and for packet forwarding on the Intranet/ISP. This requires a link between the GGSN and an address allocation server, such as AAA, or DHCP, belonging to the Intranet/ISP;

- the communication between the Packet Domain and the Intranet/ISP may be performed over any network, even an insecure e.g. the Internet. In case of an insecure connection between the GGSN and the Intranet/ISP there may be a specific security protocol in between. This security protocol is defined by mutual agreement between PLMN operator and Intranet/ISP administrator.

The following description bullet items describe the signal flow.

1) The TE sends an AT-command to the MT to set up parameters.

2) The MT sends the Activate PDP context request message to the SGSN which sends the Create PDP context request message to the chosen GGSN.

3) The GGSN deduces from the APN:

 - the server(s) to be used for address allocation and authentication;

 - the protocol such as RADIUS, DHCP or L2TP to be used with this / those server(s);

 - the communication and security feature needed to dialogue with this / those server(s) e.g. tunnel ,IPSec security association, dial-up connection (using possibly PPP).

 As an example the GGSN may use one of the following options:

 - RADIUS for authentication and IP-address allocation. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN;

 - RADIUS for authentication and DHCP for host configuration and address allocation. The AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the GGSN. After a successful authentication, the DHCP client discovers the DHCP server(s) in the ISP/Intranet and receives host configuration data;

 - L2TP for forwarding PPP frames to a L2TP Network Server.

4) The GGSN sends back to the SGSN a Create PDP Context Response message.

5) Depending on the cause value received in the Create PDP Context Response the SGSN may either send the Activate PDP Context Accept message or send the Activate PDP Context Reject message to the MS.

6) The MT responds with an AT-response that may indicate whether the context activation was successful or not. In the case of a non-successful context activation the response may also indicate the cause.

 In case of a successful context activation, the TE will start its PPP protocol after the LLC link has been established. The LCP, Authentication and NCP negotiations are then carried out. During these negotiations the GGSN may acknowledge values, for any LCP options related to 'L2' framing (e.g. 'ACCM', 'ACFC' and 'FCS-Alternatives'), as proposed by the MT, which itself is forwarding these negotiations from the TE.

NOTE: With the <PDP Type>"PPP" the MT may provide a PPP relay (or proxy) function between the TE and GGSN. This gives the opportunity for the MT to intercept the 'L2' framing end to end negotiations.

EXAMPLE: In the following example the successful PDP context activation is shown.

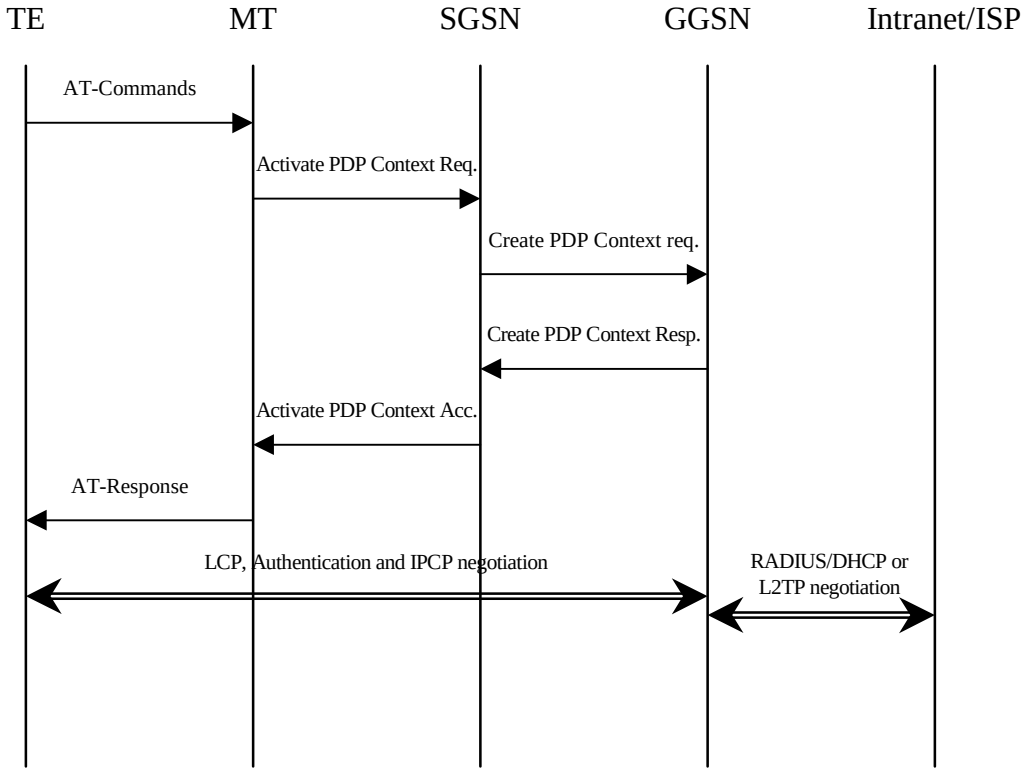


Figure 16a

13 Interworking with PDN (DHCP)

13.1 General

In current LAN environments the most commonly used configuration protocol is DHCP (Dynamic Host Configuration Protocol, RFC 2131 [26]) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6, RFC 3315 [46]). It provides a mechanism for passing a large set of configuration parameters to hosts connected to a TCP/IP network (IP address, sub-net mask, domain name, MTU, etc.) in an automatic manner. Moreover DHCP may assign IP addresses to clients for a finite lease time, allowing for sequential reassignment of addresses to different users.

The lease time is chosen by the administrator of the DHCP server (in the external network), and is therefore out of the scope of the present document.

The Packet Domain offers the end user the possibility to run DHCP end-to-end the same way as he does when connected directly to a LAN (e.g. an enterprise Intranet). No modifications should be required in common implementations of DHCP clients and servers. However a Packet Domain-specific DHCP relay agent RFC 1661 [21a] and RFC 1662 [21b] is needed in the GGSN so as to allow correct routing of DHCP requests and replies between the TE and the DHCP servers.

At PDP context activation no IP address is allocated, this is done afterwards through DHCP. After the TE's configuration has been completed by DHCP, the PDP context is updated by means of the GGSN-initiated PDP Context Modification Procedure in order to reflect the newly assigned IP address.

In the following cases the corresponding PDP context shall be deactivated and the whole procedure starting with PDP context activation shall be restarted by the MS

- if the DHCP lease expires;
- if the DHCP renewal is rejected by the DHCP server;
- if the IP address is changed during the renewal process. Usually when the lease is renewed, the IP address remains unchanged. However, if for any reason (e.g. poor configuration of the DHCP server), a different IP address is allocated during the lease renewal process the PDP Context shall be deactivated.

13.2 PDN Interworking Model for DHCP

A DHCP relay agent shall be located in the GGSN used for interworking with the IP network as illustrated in the following figure 16b.

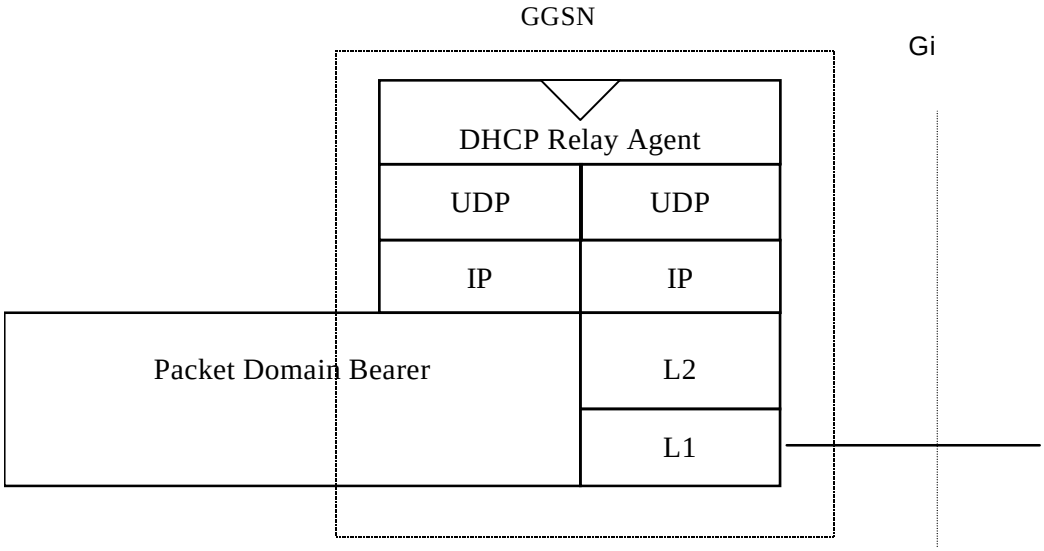


Figure 16b: The protocol stacks for the Gi IP reference point for DHCP

The DHCP relay agent relays the requests received from the DHCP client to the DHCP server(s), and the replies received from the server(s) to the corresponding client. The DHCP relay agent allows for the replies from DHCP servers to be delivered to the correct terminal, as the logical connection from the MT terminates in the GGSN, and consequently only the GGSN holds enough information to locate the DHCP client. How the DHCP relay agent identifies the MT based on the DHCP messages is out of the scope of UMTS standardisation.

DHCP provides mechanisms for user authentication and integrity protection, but does not offer any message confidentiality, therefore additional mechanisms (e.g. IPsec tunnel) may be provided if the link towards the external network is not secure. However this is out of the scope of the present document.

Apart from the particulars mentioned above, this model is basically the same as the one for interworking with IP networks described elsewhere in the present document. Using DHCP corresponds to the transparent access case as the GGSN does not take part in the functions of authentication, authorisation, address allocation, etc.

13.2.1 Address allocation by the Intranet or ISP

The MS is given an address belonging to the Intranet/ISP addressing space. The address is given dynamically immediately after the PDP context activation. This address is used for packet forwarding between the Intranet/ISP and the GGSN and within the GGSN.

The MS may authenticate itself to the Intranet/ISP by means of the relevant DHCP procedures (see RFC 3118 [45]).

The protocol configuration options are retrieved from the DHCP server belonging to the Intranet/ISP.

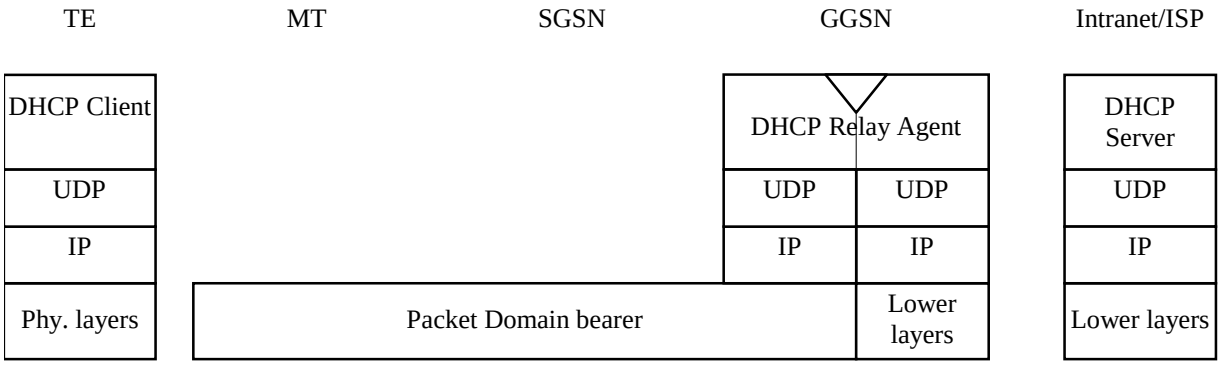


Figure 16c: Protocol stack for access with DHCP end-to-end

13.2.1.1 Address allocation using DHCPv4

The following description bullet items describe the DHCPv4 signal flow. For a detailed description of the DHCP messages refer to RFC 2131 [26] and RFC 1542 [27]. The end-to-end protocol configuration is depicted in figure 16c.

1) The TE and MT exchange several AT commands carrying the QoS and other parameters requested by the TE, and requesting the activation of a PDP context of PDP type IP. The TE selects the APN of the configured Intranet/ISP offering a DHCP service, or the APN consisting of the Reserved Service Label for DHCP that the user has subscribed to. In the latter case the TE will be connected to a PLMN operator-configured service provider offering a DHCP service (according to the APN selection rules).

2) The MT sends the Activate PDP Context Request message to the SGSN with an empty PDP address field.

3) The SGSN selects a GGSN based on the APN requested by the MS and sends a Create PDP Context Request message to that GGSN. The GGSN replies with a Create PDP Context Response message. If the GGSN has not been configured by the operator to use external PDN address allocation with DHCP for the requested APN, the cause shall be set to 'Service not supported'. No IP address is assigned at this point; the PDP address returned by the GGSN is set to 0.0.0.0, indicating that the IP address is not yet assigned and shall be negotiated by the TE with the Intranet/ISP after the PDP context activation procedure.

4) Depending on the cause value received in the Create PDP Context Response the SGSN sends either an Activate PDP Context Accept or an Activate PDP Context Reject back to the MT. In case of a successful activation the PDP context is established with the PDP address set to 0.0.0.0.

5) Upon reception of the Activate PDP Context Accept, the MT sends an AT response to the TE that acknowledges the completion of the PDP context activation procedure.

6) The TE sends a DHCPDISCOVER message with the IP destination address set to the limited broadcast address (all 1s). The GGSN will pass the DHCPDISCOVER to the DHCP relay agent which will relay the request to the DHCP server configured for the APN of the PDP context. If more than one DHCP server is configured for a given APN, the request will be sent to all of them. The DHCP relay agent will add enough information to the DHCPDISCOVER message to be able to relay the replies back to the MS. How this is done is out of the scope of UMTS standardisation.

7) DHCP servers receiving the DHCPDISCOVER request reply by sending a DHCPOFFER message including an offered IP address. The DHCP relay agent forwards the replies to the proper MS.

8) The TE chooses one of the possibly several DHCPOFFERs and sends a DHCPREQUEST confirming its choice and requesting additional configuration information. The relay agent relays the DHCPOFFER as explained in step 6.

9) The selected DHCP server receives the DHCPREQUEST and replies with a DHCPACK containing the configuration information requested by the TE. The DHCP relay agent relays the DHCPACK to the TE.

10) The DHCP relay agent passes the allocated IP address to the GGSN which stores it in the corresponding PDP context. The GGSN then initiates a PDP context modification procedure by sending an Update PDP Context Request to the appropriate SGSN with the End User Address information element set to the allocated IP address.

11) The SGSN sends a Modify PDP Context Request to the MT with the allocated IP address in the PDP Address information element. The MT acknowledges by sending a Modify PDP Context Accept to the SGSN.

12) The SGSN sends an Update PDP Context Response to the GGSN. The PDP context has been successfully updated with the allocated IP address.

EXAMPLE: In the following example a successful PDP context activation with use of DHCP from end to end is shown.

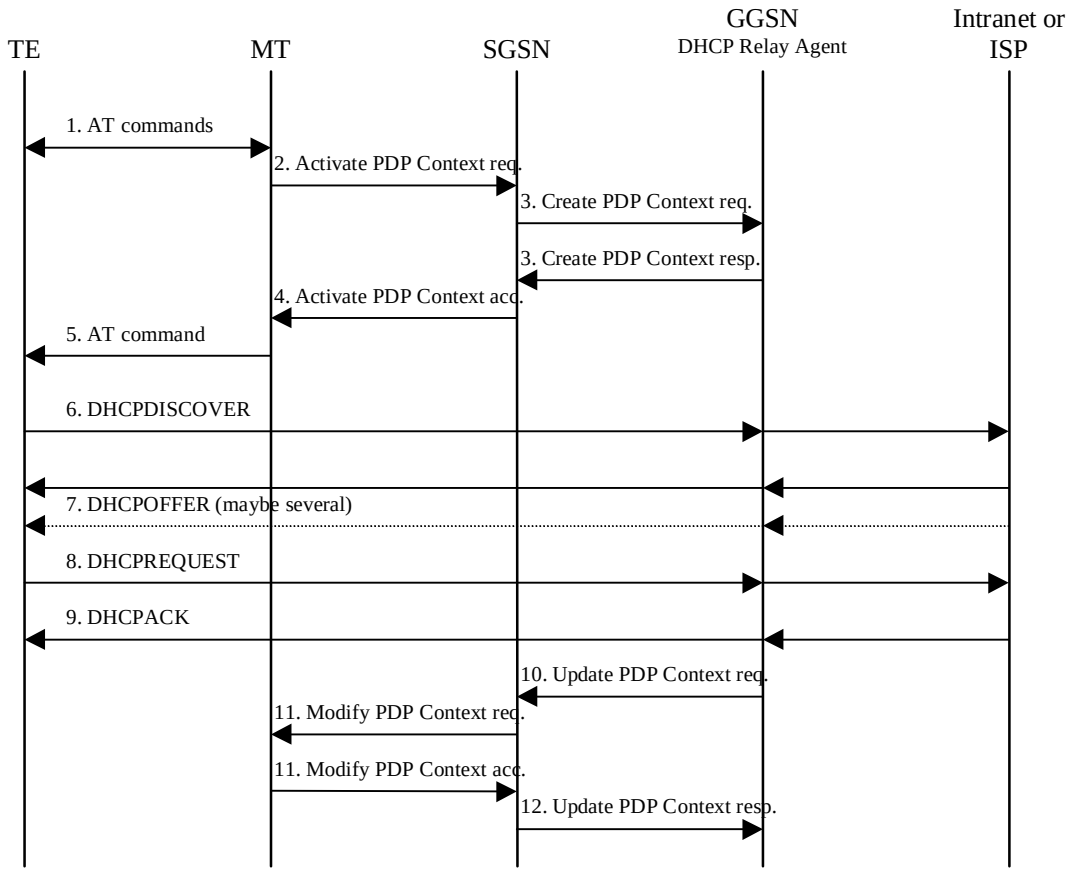


Figure 16d: DHCPv4 signal flow

13.2.1.2 Address allocation using DHCPv6

The following description bullet items describe the signal flow. For a detailed description of the DHCPv6 messages refer to the DHCPv6 IETF RFC 3315 [46]. In the context of IPv6, address allocation through DHCP is also referred to as Stateful Address Autoconfiguration. The end-to-end protocol configuration is depicted in figure 16e.

The PDP Context activation part and the initial Router Advertisement that triggers the MS to do the Stateful Address Autoconfiguration is described in subclause "IPv6 Non Transparent access to an Intranet or ISP".

1) The TE sends a SOLICIT message with the IP destination address set to the All_DHCP_Relay_Agents_and_Servers multicast address defined in the DHCPv6 IETF RFC 3315 [46]. The source address is the link local address created by the MS. The SOLICIT message shall contain one IA option.

2) The GGSN creates a RELAY-FORWARD message. The "Relay Message" option shall include the entire SOLICIT message. The GGSN sends the message to the DHCP server(s) configured for the APN using unicast addresses or All_DHCP_Servers multicast address. More details on the parameters for the RELAY-FORWARD are found in the DHCPv6 IETF RFC 3315 [46]. The GGSN may store a PDP Context ID in the Interface-Id option if this aids it in handling the Relay-Reply (the DHCP server will echo the Interface-Id option).

3) DHCP servers receiving the RELAY-FORWARD message including the SOLICIT request reply by sending a RELAY-REPLY message. The "Relay Message" option includes the ADVERTISE message with an offered IP address.

4) GGSN extracts the ADVERTISE messages and forwards the messages to the proper MS.

5) The TE chooses one of the possibly several ADVERTISE messages and sends a REQUEST confirming its choice and requesting additional configuration information.

6) GGSN embeds the REQUEST in the "Relay Message" option of the RELAY-FORWARD and sends it as explained in step 2.

7) The selected DHCP server receives the RELAY-FORWARD and replies with a RELAY-REPLY. The "Relay Message" option includes the REPLY message containing the configuration information requested by the TE.

8) The GGSN extracts the REPLY message and forwards it to the proper MS. GGSN also extracts IA option information such as the allocated MS IPv6 address and its lifetime and stores it in the corresponding PDP context. The GGSN shall silently discard any Neighbour Solicitation message sent by the MS to perform Duplicate Address Detection (see 3GPP TS 23.060 [3]).

9) The GGSN initiates a PDP context modification procedure by sending an Update PDP Context Request to the appropriate SGSN with the End User Address information element set to the allocated IPv6 address.

10) The SGSN sends a Modify PDP Context Request to the MT with the allocated IPv6 address in the PDP Address information element.

11) The MT acknowledges by sending a Modify PDP Context Accept to the SGSN.

12) The SGSN sends an Update PDP Context Response to the GGSN. The PDP context has been successfully updated with the allocated IPv6 address.

13) In the Stateful Address Autoconfiguration, Router Advertisements sent by GGSN on the MS-GGSN link shall not contain any Prefix Information option, even when GGSN has knowledge of the Prefix of the MS through the DHCP relay agent. The Prefix need not be advertised since the MS is the only host on the link and Stateless Address Autoconfiguration shall not be performed concurrently to Stateful Address Autoconfiguration.

EXAMPLE: In the following example a successful PDP context activation with use of DHCPv6 from end to end is shown.

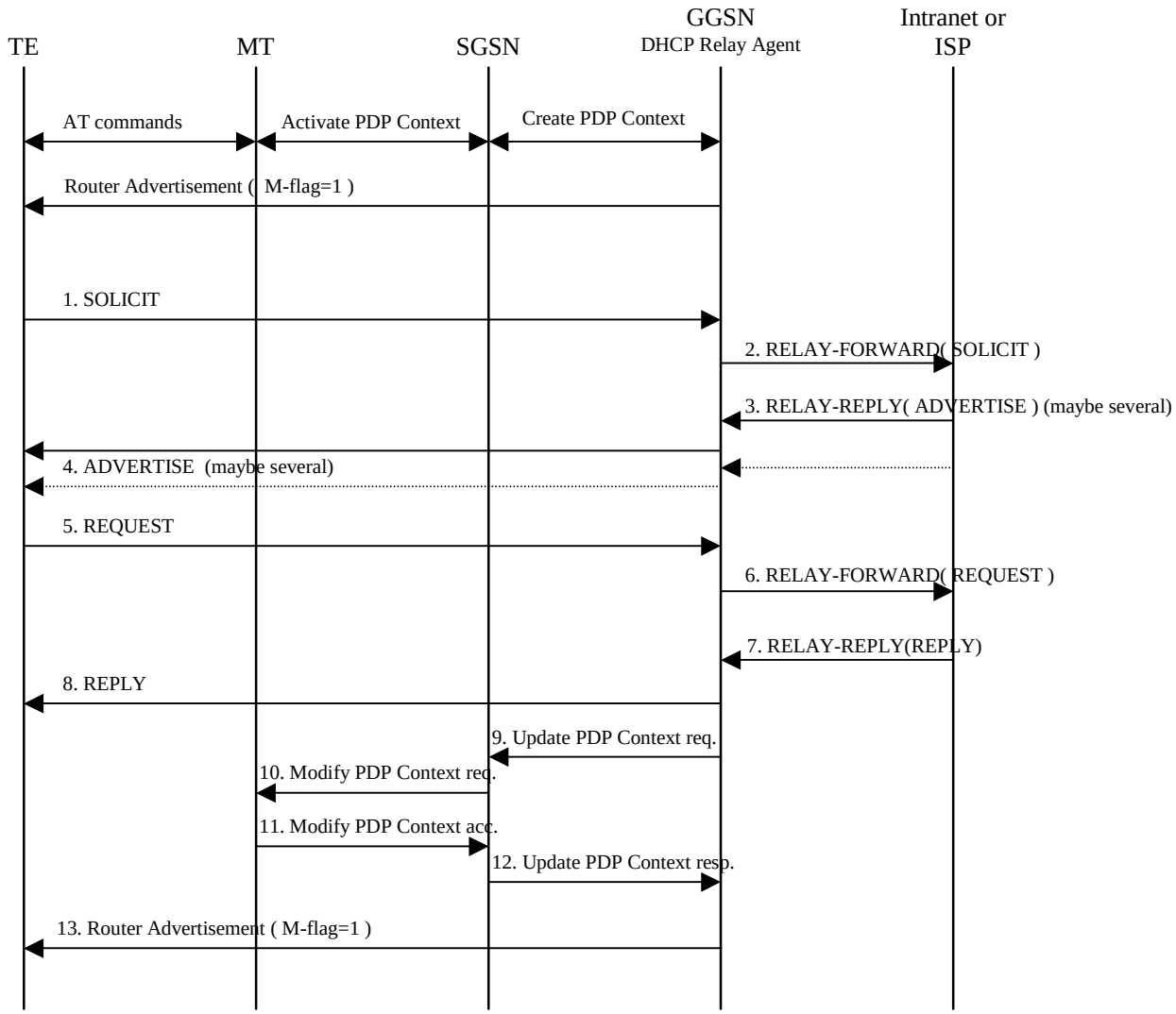


Figure 16e: DHCPv6 signal flow

13.2.2 Other configuration by the Intranet or ISP (IPv6 only)

When using IPv6, in some situations the MS may need additional configuration information from the Intranet or ISP besides the IP address. It may for example be IMS related configuration options (see 3GPP TS 24.229 [47]). If the MS is DHCP capable and the IPv6 address has been allocated using Stateless Address Autoconfiguration, the MS may use a procedure as in the example below to configure additional external network protocol parameters, or other parameters that apply to the Intranet or ISP. The GGSN shall in this case indicate to the MS that there is additional configuration information to retrieve by setting the O-flag in the Router Advertisements. This shall be configured per APN in the GGSN.

The following description bullet items describe an example of a signal flow, where the MS directs an Information-Request to the All_DHCP_Relay_Agents_and_Servers multicast address. The MS may also direct the message to a specific server instead of all servers. For a detailed description of the DHCPv6 messages refer to the DHCPv6 IETF RFC 3315 [46]. The sequence is depicted in figure 16f.

1) A Router Advertisement with the O-flag set, is sent from GGSN to TE to indicate to it to retrieve other configuration information.

2) The TE sends an INFORMATION-REQUEST message with the IP destination address set to the All_DHCP_Relay_Agents_and_Servers multicast address defined in the DHCPv6 IETF RFC 3315 [46]. The source address shall be the link-local address of the MS. The DHCP relay agent in the GGSN shall forward the message.

3) DHCP servers receiving the forwarded INFORMATION-REQUEST message, reply by sending a RELAY-REPLY message, with the "Relay Message" option including a REPLY message with the requested configuration parameters.

The TE chooses one of the possibly several REPLY messages and extracts the configuration information.

EXAMPLE: In the following example a request for information with use of DHCPv6 from end to end is shown.

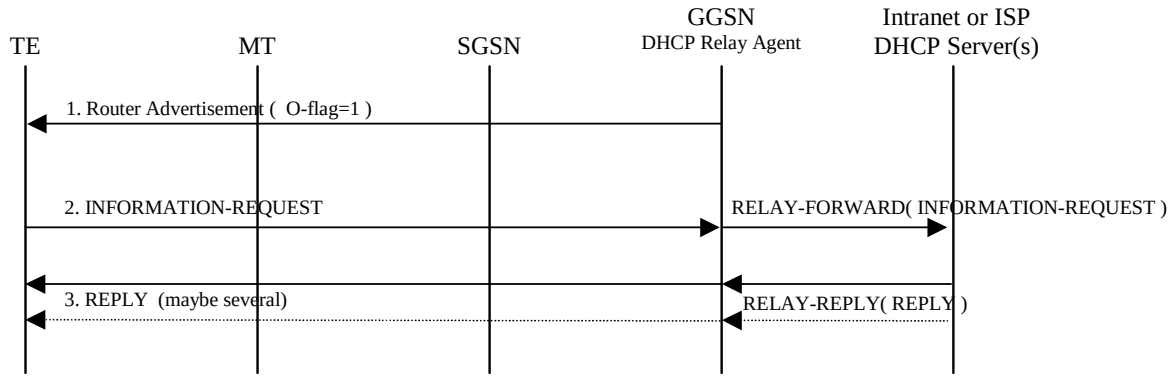


Figure 16f: DHCPv6 Other configuration signal flow

14 Internet Hosted Octet Stream Service (IHOSS)

Figure 17: Void

Figure 18: Void

Figure 19: Void

Figure 20: Void

15 Interworking between Packet Domains

The primary reason for the interworking between Packet Domains is to support roaming subscribers as described in 3GPP TS 23.060 [3]. The general model for Packet Domain interworking is shown in figure 21.

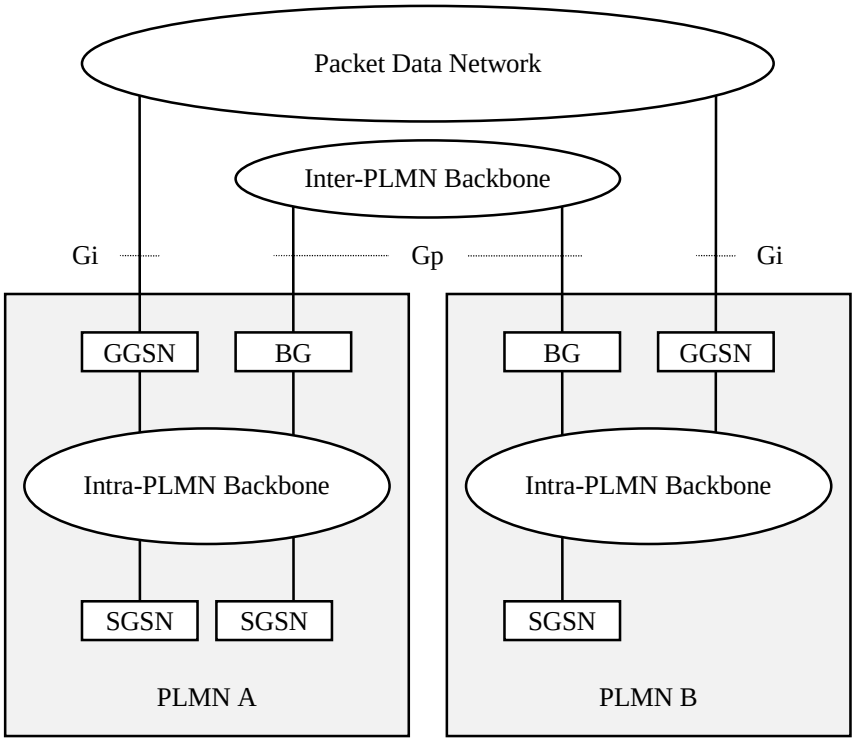


Figure 21: General interworking between Packet Domains to support roaming subscribers.

For roaming subscribers that have a PDP address allocated from the HPLMN a forwarding route between the HPLMN and the VPLMN is created. This route is used for both mobile terminated and mobile originated data traffic. The communication is done via the BGs (Border Gateways) as described in 3GPP TS 23.060 [3].

The procedures to set the link between the SGSN in the VPLMN and the GGSN in the HPLMN are described in 3GPP TS 23.060 [3].

The inter-PLMN link may be any packet data network or dedicated link as described in 3GPP TS 23.060 [3]. The PLMN operators may have a dedicated inter-PLMN link to fulfil the QoS requirements of a certain protocol.

15.1 Security Agreements

Each PLMN operator may support IPsec (RFC 1825 [54]) and accompanying specifications for authentication (RFC 1826 [55]) and encryption (RFC 1827 [56]) as a basic set of security functionality in its border gateways. The PLMN operators may decide to use other security protocols based on bilateral agreements.

15.2 Routing protocol agreements

Each PLMN operator may support BGP (RFC 1771 [53]) as a basic set of routing functionality in its border gateways. The PLMN operators may decide to use other routing protocols based on bilateral agreements.

15.3 Charging agreements

Sharing the cost of the inter-PLMN link is subject to the agreement between the PLMN operators.

There may be a requirement to collect charging information in the Border Gateway (see figure 21) and this is down to the normal interconnect agreement between PLMN and PDN operators.

16 Usage of RADIUS on Gi interface

A GGSN may, on a per APN basis, use RADIUS authentication to authenticate a user and RADIUS accounting to provide information to an AAA (Authentication, Authorization and Accounting) server.

16.1 RADIUS Authentication

RADIUS Authentication shall be used according to RFC 2865 [38] and RFC 3162 [50].

The RADIUS client function may reside in a GGSN. When the GGSN receives a Create PDP Context request message the RADIUS client function may send the authentication information to an authentication server, which is identified during the APN provisioning.

The authentication server checks that the user can be accepted. The response (when positive) may contain network information, such as an IP address or IPv6 prefix for the user.

The information delivered during the RADIUS authentication can be used to automatically correlate the users identity (the MSISDN or IMSI) to the IP-address or IPv6 prefix, assigned/confirmed by the GGSN or the authentication server respectively. The same procedure applies, in case of sending the authentication to a 'proxy' authentication server.

RADIUS Authentication is only applicable to the primary PDP context. When the GGSN receives an Access-Accept message from the authentication server it shall complete the PDP context activation procedure. If Access-Reject or no response is received, the GGSN shall reject the PDP Context Activation attempt with a suitable cause code, e.g. User Authentication failed.

16.2 RADIUS Accounting

RADIUS Accounting shall be used according to RFC 2866 [39] and RFC 3162 [50].

The RADIUS accounting client function may reside in a GGSN. The RADIUS accounting client may send information to an accounting server, which is identified during the APN provisioning. The accounting server may store this information and use it to automatically identify the user. This information can be trusted because the GPRS network has authenticated the subscriber (i.e. SIM card and possibly other authentication methods).

RADIUS Accounting-Request Start and Stop messages may be used during both primary and secondary PDP context activation and deactivation procedures respectively.

The use of Accounting-Request STOP and in addition the Accounting ON and Accounting OFF messages may be used to ensure that information stored in the accounting server is synchronised with the GGSN information.

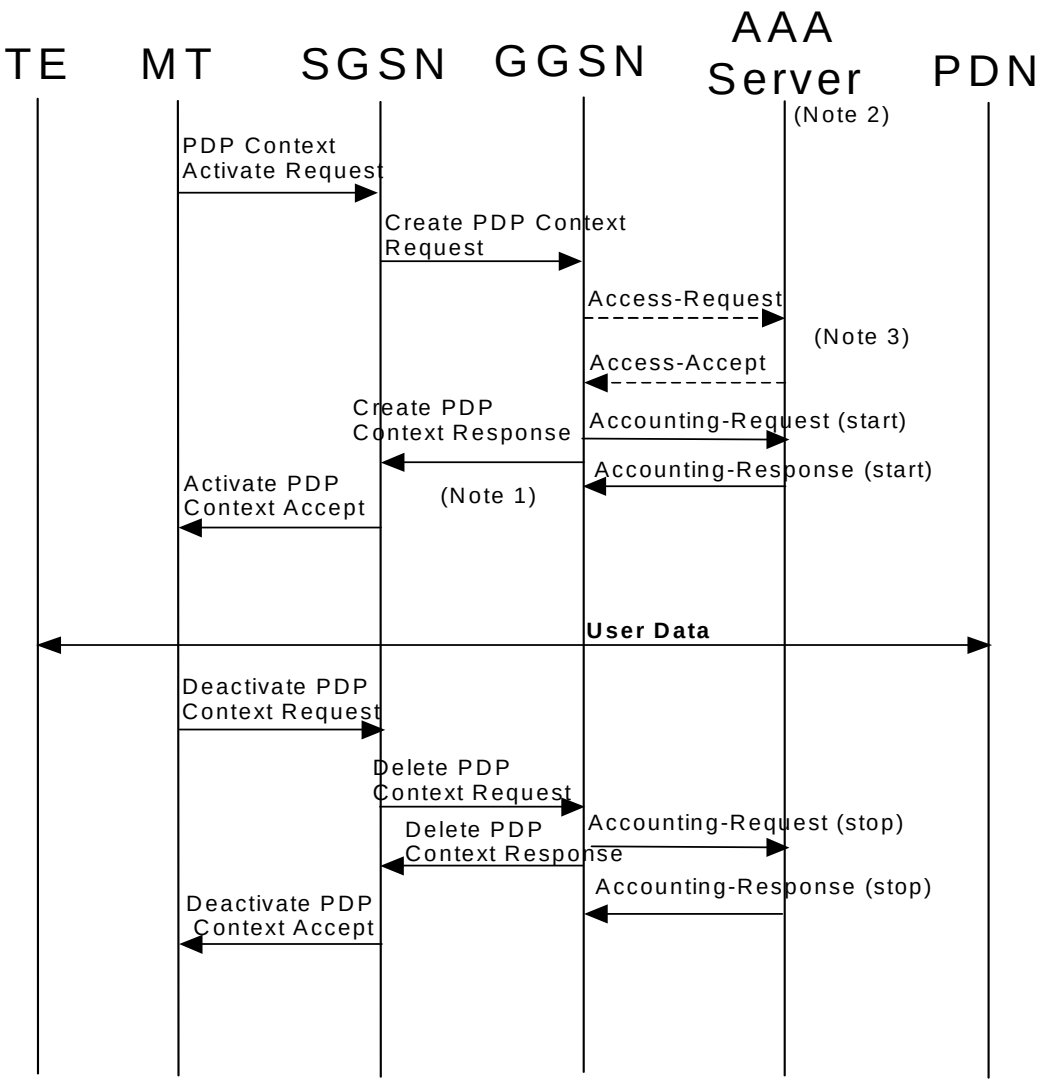
If the AAA server is used for IP address or IPv6 prefix assignment, then, upon reception of a RADIUS Accounting-Request STOP message for all PDP contexts associated to a session defined by APN and IMSI or MSISDN, the AAA server may make the associated IP address or IPv6 prefix available for assignment.

In order to avoid race conditions, the GGSN shall include a 3GPP Vendor-Specific sub-attribute "Session Stop indicator" when it sends the Accounting-Request STOP for the last PDP context of a PDP session and the PDP session is terminated (i.e. the IP address or IPv6 prefix and all GTP tunnels can be released). The AAA server shall not assume the PDP session terminated until an Accounting-Request STOP with the Session Stop indicator is received.

16.3 Authentication and accounting message flows

16.3.1 IP PDP type

Figure 22 represents the RADIUS message flows between a GGSN and an Authentication, Authorization and Accounting (AAA) server.



NOTE 1: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may wait for the Accounting Response (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting Response (START) is not received.
NOTE 2: Separate accounting and authentication servers may be used.
NOTE 3: The Access-Request message shall be used for primary PDP context only.
NOTE 4: The Accounting-Request (Start) message may be sent at a later stage, e.g. after IPv6 address has been assigned and PDP Context updated, in case of a stateful address autoconfiguration.

Figure 22: RADIUS message flow for PDP type IP (successful user authentication case)

When a GGSN receives a Create PDP Context Request message for a given APN, the GGSN may (depending on the configuration for this APN) send a RADIUS Access-Request to an AAA server. The AAA server authenticates and authorizes the user. If RADIUS is also responsible for IP address or IPv6 prefix allocation the AAA server shall return the allocated IP address or IPv6 prefix in the Access-Accept message.

Even if the GGSN was not involved in user authentication (e.g. transparent network access mode), it may send a RADIUS Accounting-Request START message to an AAA server. This message contains parameters, e.g. the tuple which includes the user-id and IP address or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the AAA server that the user session has started.

At a stateful address autoconfiguration, no IP address or IPv6 prefix is available at PDP context activation. In that case the GGSN may wait to send the Accounting-Request START message until the TE receives its IP address in a DHCP-REPLY.

If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may wait for the Accounting Response (START) before sending the CreatePDPContextResponse. The GGSN may reject the PDP context if the Accounting Response (START) is not received. The authentication and accounting servers may be separately configured for each APN.

When the GGSN receives a Delete PDP Context Request message and providing a RADIUS Accounting-Request START message was sent previously, the GGSN shall send a RADIUS Accounting-Request STOP message to the AAA server, which indicates the termination of this particular user session. The GGSN shall immediately send a Delete PDP context response, without waiting for an Accounting-Response STOP message from the AAA server.

The AAA server shall deallocate the IP address or IPv6 prefix (if any) initially allocated to the subscriber, if there is no session for the subscriber.

Accounting-Request ON and Accounting-Request OFF messages may be sent from the GGSN to the AAA server to ensure the correct synchronization of the session information in the GGSN and the AAA server.

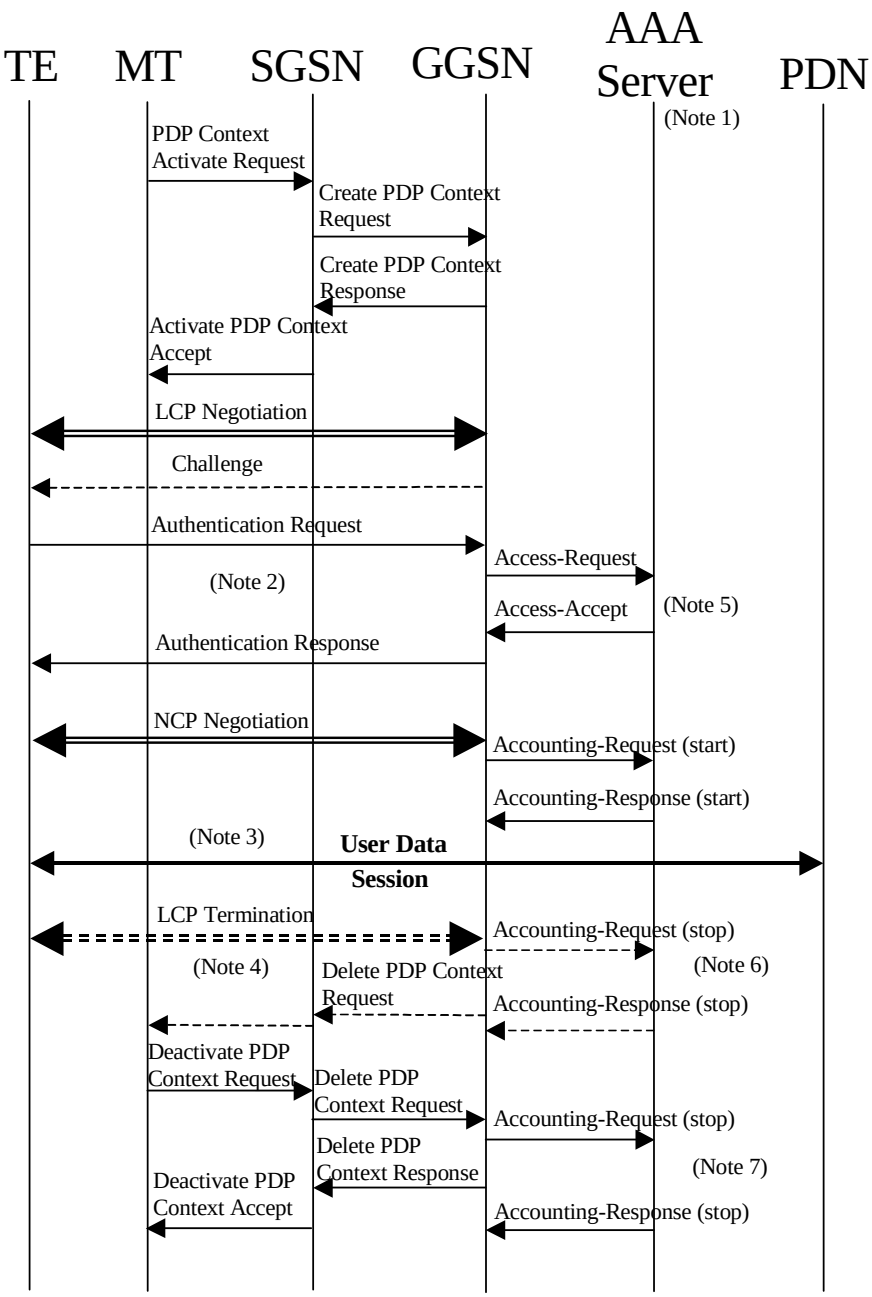
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

Prior to a scheduled restart, the GGSN may send Accounting-Request OFF message to the AAA server. The AAA server may then release the associated resources.

If an Access-Challenge is sent to the GGSN when an Access-Request message is pending and when IP PDP type is used, the GGSN shall silently discard the Access-Challenge message and it shall treat an Access-Challenge as though it had received an Access-Reject instead RFC 2865 [38].

16.3.2 PPP PDP type

Figure 23 describes the RADIUS message flows between a GGSN and an Authentication, Authorization and Accounting (AAA) server for the case where PPP is terminated at the GGSN. The case where PPP is relayed to an LNS is beyond the scope of the present document.



NOTE 1: Separate accounting and Authentication servers may be used.
NOTE 2: Actual messages depend on the used authentication protocol (e.g. PAP, CHAP).
NOTE 3: If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may delete the PDP context if the Accounting Response (START) is not received.
NOTE 4: An LCP termination procedure may be performed. Either the MS or the GGSN may initiate the context deactivation.
NOTE 5: The Access-Request message shall be used for primary PDP context only.
NOTE 6: Network Initiated deactivation.
NOTE 7: User Initiated deactivation.

Figure 23: RADIUS message flow for PDP type PPP (successful user authentication case)

When a GGSN receives a Create PDP Context Request message for a given APN, the GGSN shall immediately send a Create PDP context response back to the SGSN. After PPP link setup, the authentication phase may take place. During Authentication phase, the GGSN sends a RADIUS Access-Request to an AAA server. The AAA server authenticates and authorizes the user. If RADIUS is also responsible for IP address allocation the AAA server shall return the allocated IP address or IPv6 prefix in the Access-Accept message (if the user was authenticated).

If the user is not authenticated, the GGSN shall send a Delete PDP context request to the SGSN.

Even if the GGSN was not involved in user authentication (e.g. for PPP no authentication may be selected), it may send a RADIUS Accounting-Request START message to an AAA server. This message contains parameters, e.g. a tuple which includes the user-id and IP address or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message also indicates to the AAA server that the user session has started, and the QoS parameters associated to the session.

If some external applications require RADIUS Accounting request (Start) information before they can process user packets, then the selected APN (GGSN) may be configured in such a way that the GGSN drops user data until the Accounting Response (START) is received from the AAA server. The GGSN may delete the PDP context if the Accounting Response (START) is not received. The Authentication and Accounting servers may be separately configured for each APN.

When the GGSN receives a Delete PDP Context Request message and providing a RADIUS Accounting-Request START message was sent previously, the GGSN shall send a RADIUS Accounting-Request STOP message to the AAA server, which indicates the termination of this particular user session. The GGSN shall immediately send a Delete PDP context response, without waiting for an Accounting-Response STOP message from the AAA server.

The AAA server shall deallocate the IP address or IPv6 prefix (if any) initially allocated to the subscriber.

Accounting-Request ON and Accounting-Request OFF messages may be sent from the GGSN to the AAA server to ensure the correct synchronization of the session information in the GGSN and the AAA server.

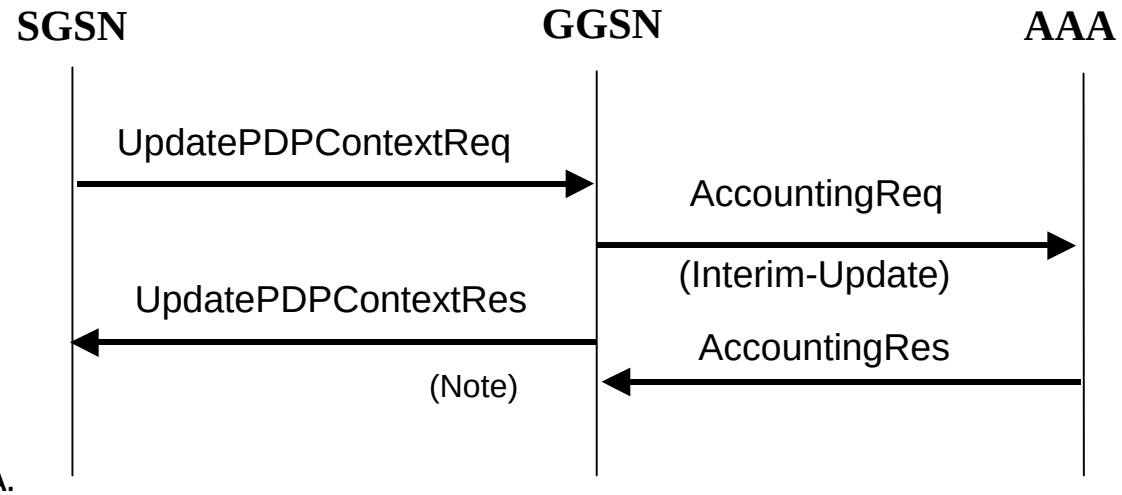
The GGSN may send an Accounting-Request ON message to the AAA server to indicate that a restart has occurred. The AAA server may then release the associated resources.

Prior to a scheduled restart, the GGSN may send Accounting-Request OFF message to the AAA server, the AAA server may then release the associated resources.

If an Access-Challenge is sent to the GGSN when using PPP PDP type, the GGSN shall handle it by PPP CHAP providing PPP CHAP was the selected Authentication protocol. If CHAP authentication was not selected, authentication shall fail RFC 2865 [38].

16.3.3 Accounting Update

During the life of a PDP context some information related to this PDP context may change (i.e. SGSN address if a Inter-SGSN RA update occurs). Upon reception of an UpdatePDPContextRequest from the SGSN, the GGSN may send an Accounting Request Interim-Update to the AAA server to update the necessary information related to this PDP context (see figure 24). In such a case, the GGSN need not wait for the RADIUS AccountingResponse from the AAA server message before sending the UpdatePDPContextResponse to the SGSN. The GGSN may delete the PDP context if the AccountingResponse is not received from the



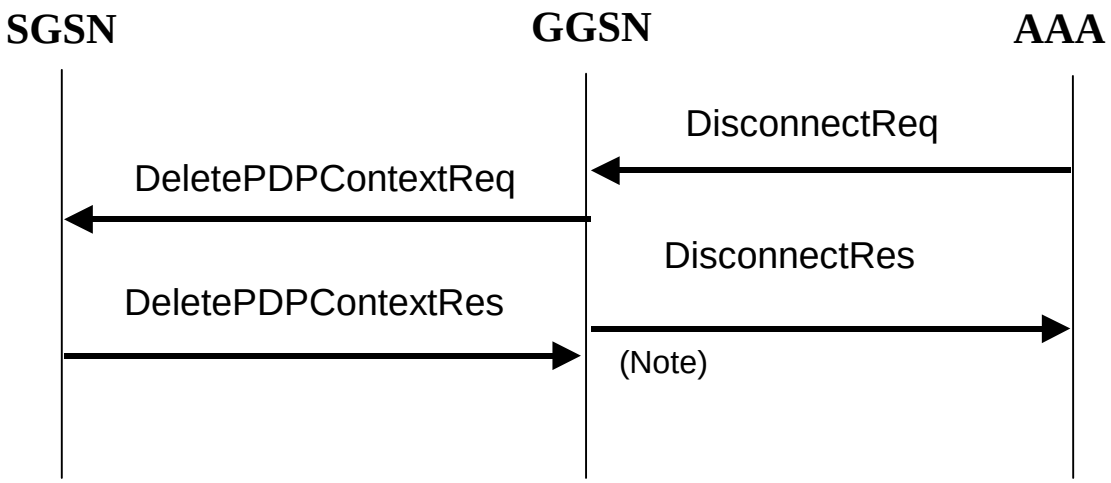
AAA.

NOTE: As shown the GGSN need not wait for the RADIUS AccountingResponse from the AAA server message to send the UpdatePDPContextResponse to the SGSN. The GGSN may delete the PDP context if the AccountingResponse is not received from the AAA.

Figure 24: RADIUS for PDP context Update

16.3.4 AAA-Initiated PDP context termination

RADIUS is used as the protocol between the GGSN and a AAA server or proxy for applications (e.g. MMS) to deliver information related to GPRS user session. However some IP applications could need to interwork with the GGSN to terminate a particular PDP context. For this purpose, the AAA server or proxy may send a RADIUS Disconnect Request to the GGSN. As depicted in figure 25, the GGSN may react by deleting the corresponding PDP context or silently discard the Disconnect Request message. For more information on RADIUS Disconnect, see RFC 2882 [41]. If the GGSN deletes the corresponding PDP context, it need not wait for the DeletePDPContextResponse from the SGSN before sending the RADIUS DisconnectResponse to the AAA server.



NOTE: As showed on Figure 25, the GGSN need not wait for the DeletePDPContextResponse from the SGSN to send the RADIUS DisconnectResponse to the AAA server.

Figure 25: PDP Context deletion with RADIUS

16.4 List of RADIUS attributes

The following tables describe the actual content of the RADIUS messages exchanged between the GGSN and the AAA server. Other RADIUS attributes may be used as defined in RADIUS RFC(s). Unless otherwise stated, when the encoding scheme of an attribute is specified as UTF-8 encoding, this shall be interpreted as UTF-8 hexadecimal encoding.

16.4.1 Access-Request message (sent from the GGSN to AAA server)

Table 1 describes the attributes of the Access-Request message.

Table 1: The attributes of the Access-Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username is provided by the user (extracted from the Protocol Configuration Options (PCO) field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present.	String	Mandatory
2	User-Password	User password provided by the user if PAP is	String	Conditional

Attr #	Attribute Name	Description	Content	Presence Requirement
		used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no password is available a generic password, configurable on a per APN basis, shall be present.		Note 1
3	CHAP-Password	User password provided by the user if CHAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used).	String	Conditional Note 2
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 3 and 4
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 3 and 4
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 2
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	IP address allocated for this user	IPv4	Conditional Note 4
9	Framed-IP-Netmask	Netmask for the user IP address	IPv4	Conditional Note 4
97	Framed-IPv6-Prefix	IPv6 address prefix allocated for this user	IPv6	Conditional Note 4
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 4 and 5
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded decimal. (Note 6).	Optional
60	CHAP-Challenge	Challenge if CHAP is used (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used).	String	Conditional Note 2
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according subclause 16.4.7	See subclause 16.4.7	Optional except sub-attribute 3 which is conditional

NOTE 1: Shall be present if PAP is used.
NOTE 2: Shall be present if CHAP is used.
NOTE 3: Either NAS-IP-Address or NAS-Identifier shall be present.
NOTE 4: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different.
NOTE 5: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.
NOTE 6: There are no leading characters in front of the country code.

16.4.2 Access-Accept (sent from AAA server to GGSN)

Table 2 describes the attributes of the Access-Accept message. See RFC 2548 [51] for definition of MS specific attributes.

Table 2: The attributes of the Access-Accept message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username received in the Access-Request message or a substitute username provided by the AAA server. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed-Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	IP address allocated for this user, if the AAA server is used to allocate IP address.	IPv4	Conditional Note 3
9	Framed-IP-Netmask	Netmask for the user IP address, if the AAA server is used to allocate IP netmask.	IPv4	Conditional Note 2
97	Framed-IPv6-Prefix	IPv6 address prefix allocated for this user, if the AAA server is used to allocate IP address prefixes.	IPv6	Conditional Note 2
100	Framed-IPv6-Pool	Name of the prefix pool for the specific APN	IPv6	Optional Note 2
12	Framed-IP-MTU	MTU for the user towards this particular APN, MTU shall be less or equal to 1500	String	Optional
25	Class	Identifier to be used in all subsequent accounting messages.	String	Optional (Note 1)
27	Session-Timeout	Indicates the timeout value (in seconds) for the user session	32 bit unsigned Integer	Optional
28	Idle-Timeout	Indicates the timeout value (in seconds) for idle user session	32 bit unsigned Integer	Optional
26/311	MS- Primary-DNS-server	Contains the primary DNS server address for this APN	IPv4	Optional Note 3
26/311	MS-Secondary-DNS-Server	Contains the secondary DNS server address for this APN	IPv4	Optional Note 3
26/311	MS-Primary-NBNS-Server	Contains the primary NetBios name server address for this APN	IPv4	Optional Note 3
26/311	MS-Secondary-NBNS-Server	Contains the secondary NetBios server address for this APN	IPv4	Optional Note 3
26/10415/17	3GPP-IPv6-DNS-Servers	List of IPv6 addresses of DNS servers for this APN	IPv6	Optional Note 3
NOTE 1: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message NOTE 2: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE 3: Either IPv4 or IPv6 address attribute shall be present.				

16.4.3 Accounting-Request START (sent from GGSN to AAA server)

Table 3 describes the attributes of the Accounting-Request START message.

Table 3: The attributes of the Accounting-Request START message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	GGSN IP address for communication with the	IPv4	Conditional

Attr #	Attribute Name	Description	Content	Presence Requirement
		AAA server.		Notes 1 and 3
95	NAS-IPv6-Address	GGSN IPv6 address for communication with the AAA server.	IPv6	Conditional Notes 1 and 3
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 3
97	Framed-IPv6-Prefix	User IPv6 Prefix	IPv6	Conditional Note 3
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 3 and 4
25	Class	Received in the access accept	String	Conditional (Note 2)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded decimal. (Note 6)	Optional
40	Acct-Status-Type	Type of accounting message	START	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time (in seconds) of the event generating this Accounting-Request.	32 unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. (Note 5)	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according subclause 16.4.7.	See subclause 16.4.7	Optional except sub-attribute 3 which is conditional

NOTE 1: Either NAS-IP-Address or NAS-Identifier shall be present.
NOTE 2: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message
NOTE 3: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different.
NOTE 4: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.
NOTE 5: The GGSN IP address is the same as that used in the GCDRs.
NOTE 6: There are no leading characters in front of the country code.

16.4.4 Accounting Request STOP (sent from GGSN to AAA server)

Table 4 describes the attributes of the Accounting-Request STOP message.

Table 4: The attributes of the Accounting-Request STOP message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 1 and 3
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and 3
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 3
97	Framed-IPv6-Prefix	User IPv6 Prefix	IPv6	Conditional Note 3
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 3 and 4
25	Class	Received in the access accept	String	Optional (Note 2)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded. (Note 6).	Optional
40	Acct-Status-Type	Indicates the type of accounting request	STOP	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time of the event generating this Accounting-Request	Second	Optional
42	Acct-Input-Octets	GGSN counted number of octets sent by the user for the PDP context	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN counted number of octets received by the user for the PDP context	32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. (Note 5)	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or LOCAL	Optional
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN counted number of packets received by the user	Packet	Optional

Attr #	Attribute Name	Description	Content	Presence Requirement
49	Acct-Terminate-Cause	Indicate how the session was terminated	See RFC 2866 [39]	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according to subclause 16.4.7.	See subclause 16.4.7	Optional except sub-attribute 3 which is conditional
NOTE 1: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message NOTE 3: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different. NOTE 4: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address. NOTE 5: The GGSN IP address is the same as that used in the GCDRs. NOTE 6: There are no leading characters in front of the country code.				

16.4.5 Accounting Request ON (optionally sent from GGSN to AAA server)

Table 5 describes the attributes of the Accounting-Request ON message.

Table 5: The attributes of the Accounting-Request ON message

Attr #	Attribute Name	Description	Content	Presence Requirement
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 1 and 2
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and 2
30	Called-Station-ID	Identifier for the target network.	APN (UTF-8 encoded)	Optional
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1
NOTE 1: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2: Either IPv4 or IPv6 address attribute shall be present.				

16.4.6 Accounting Request OFF (optionally sent from GGSN to AAA server)

Table 6 describes the attributes of the Accounting-Request OFF message.

Table 6: The attributes of the Accounting-Request OFF message

Attr #	Attribute Name	Description	Content	Presence Requirement
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 1 and 2
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and 2
30	Called-Station-ID	Identifier for the target network.	APN (UTF-8 encoded)	Optional
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1
NOTE 1: Either NAS-IP-Address or NAS-Identifier shall be present. NOTE 2: Either IPv4 or IPv6 address attribute shall be present.				

16.4.7 Sub-attributes of the 3GPP Vendor-Specific attribute

Table 7 describes the sub-attributes of the 3GPP Vendor-Specific attribute of the Access-Request, Accounting-Request START, Accounting-Request STOP and Accounting-Request Interim-Update messages.

Table 7: The sub-attributes of the 3GPP Vendor-Specific attribute of the Access-Request, Accounting-Request START, Accounting-Request STOP and Accounting-Request Interim-Update messages

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
1	3GPP-IMSI	IMSI for this user	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
2	3GPP-Charging-Id	Charging ID for this PDP Context (this together with the GGSN-Address constitutes a unique identifier for the PDP context).	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
3	3GPP-PDP Type	Type of PDP context, e.g. IP or PPP	Conditional (mandatory if attribute 7 is present)	Access-Request Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
4	3GPP-CG-Address	Charging Gateway IP address	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
5	3GPP-GPRS-Negotiated-QoS-Profile	QoS profile applied by GGSN	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
6	3GPP-SGSN-Address	SGSN IP address that is used by the GTP control plane for the handling of control messages. It may be used to identify the PLMN to which the user is attached.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
7	3GPP-GGSN-Address	GGSN IP address that is used by the GTP control plane for the context establishment. It is the same as the GGSN IP address used in the GCDRs.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
8	3GPP-IMSI-MCC-MNC	MCC and MNC extracted from the user's IMSI (first 5 or 6 digits, as applicable from	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
		the presented IMSI).		Interim-Update
9	3GPP-GGSN- MCC-MNC	MCC-MNC of the network the GGSN belongs to.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
10	3GPP-NSAPI	Identifies a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP Accounting-Request Interim-Update
11	3GPP- Session-Stop-Indicator	Indicates to the AAA server that the last PDP context of a session is released and that the PDP session has been terminated.	Optional	Accounting Request STOP
12	3GPP- Selection-Mode	Contains the Selection mode for this PDP Context received in the Create PDP Context Request Message	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
13	3GPP-Charging-Characteristics	Contains the charging characteristics for this PDP Context received in the Create PDP Context Request Message (only available in R99 and later releases)	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
14	3GPP-CG-IPv6-Address	Charging Gateway IPv6 address	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
15	3GPP-SGSN-IPv6-Address	SGSN IPv6 address that is used by the GTP control plane for the handling of control messages. It may be used to identify the PLMN to which the user is attached.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
16	3GPP-GGSN-IPv6-Address	GGSN IPv6 address that is used by the GTP control plane for the context establishment.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update
17	3GPP- IPv6-DNS-Servers	List of IPv6 addresses of DNS	Optional	Access-Accept

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)
		servers for an APN		
18	3GPP-SGSN-MCC-MNC	MCC and MNC extracted from the RAI within the Create PDP Context Request or Update PDP Context Request message.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update

The RADIUS vendor Attribute is encoded as follows (as per RFC 2865 [38])

Bits

Octets	8	7	6	5	4	3	2	1
1	Type = 26							
2	Length = n							
3	Vendor id octet 1							
4	Vendor id octet 2							
5	Vendor id octet 3							
6	Vendor id octet 4							
7-n	String							

$n \geq 7$

3GPP Vendor Id = 10415

The string part is encoded as follows:

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type =							
2	3GPP Length = m							
3 –m	3GPP value							

$m \geq 2$ and $m \leq 248$

The 3GPP specific attributes encoding is clarified below.

1 **-** 3GPP-***IMSI***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 1							
2	3GPP Length= m							
3-m	IMSI digits 1-n (UTF-8 encoded)							

3GPP Type: 1

$n \leq 15$

Length: $m \leq 17$

IMSI value: Text:

This is the UTF-8 encoded IMSI; The definition of IMSI shall be in accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24]. There shall be no padding characters between the MCC and MNC, and between the MNC and MSIN. If

the IMSI is less than 15 digits, the padding in the GTP information element shall be removed by the GGSN and not encoded in this sub-attribute.

2 - 3GPP-***Charging ID***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 2							
2	3GPP Length= 6							
3	Charging ID value Octet 1							
4	Charging ID value Octet 2							
5	Charging ID value Octet 3							
6	Charging ID value Octet 4							

3GPP Type: 2

Length: 6

Charging ID value: 32 bits unsigned integer

3 - 3GPP-***PDP type***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 3							
2	3GPP Length= 6							
3	PDP type octet 1							
4	PDP type octet 2							
5	PDP type octet 3							
6	PDP type octet 4							

3GPP Type: 3

Length: 6

PDP type value: Unsigned 32 bits integer

PDP type octet possible values:

0 = IPv4

1 = PPP

2 = IPv6

4 - 3GPP-***Charging Gateway address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 4							
2	3GPP Length= 6							
3	Charging GW addr Octet 1							
4	Charging GW addr Octet 2							
5	Charging GW addr Octet 3							
6	Charging GW addr Octet 4							

3GPP Type: 4

Length: 6

Charging GW address value: Address

5 - 3GPP-***GPRS Negotiated QoS profile***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 5							
2	3GPP Length= L							
3 -L	UTF-8 encoded QoS profile							

3GPP Type: 5

Length: 27 (release 99) or 11 (release 98)

QoS profile value: Text

UTF-8 encoded QoS profile syntax:

"<Release indicator> – <release specific QoS IE UTF-8 encoding>"

<Release indicator> = UTF-8 encoded number :

"98" = Release 98

"99"= Release 99

<release specific QoS profile UTF-8 encoding> = UTF-8 encoded QoS profile for the release indicated by the release indicator.

The UTF-8 encoding of a QoS IE is defined as follows: each octet is described by 2 UTF-8 encoded digits, defining its hexadecimal representation. The QoS profile definition is in 3GPP TS 24.008 [23].

The release 98 QoS profile data is 3 octets long, which then results in a 6 octets UTF-8 encoded string,

The release 99 QoS profile data is 11 octets long, which results in a 22 octets UTF-8 encoded string.

6 - 3GPP-***SGSN address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 6							
2	3GPP Length= 6							
3	SGSN addr Octet 1							
4	SGSN addr Octet 2							
5	SGSN addr Octet 3							
6	SGSN addr Octet 4							

3GPP Type: 6

Length: 6

SGSN address value: Address

7 - 3GPP-***GGSN address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 7							
2	3GPP Length= 6							
3	GGSN addr Octet 1							
4	GGSN addr Octet 2							
5	GGSN addr Octet 3							
6	GGSN addr Octet 4							

3GPP Type: 7

Length: 6

GGSN address value: Address

8 - 3GPP-***IMSI MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 8							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 8

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

MS address value: text

This is the UTF-8 encoding of the MS MCC-MNC values. In accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

9 - 3GPP-***GGSN MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 9							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 9

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

GGSN address value: text

This is the UTF-8 encoding of the GGSN MCC-MNC values. In accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

10 - 3GPP-***NSAPI***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 10							
2	3GPP Length= 3							
3	NSAPI							

3GPP Type: 10

Length: 3

NSAPI value: text

It is the value of the NSAPI of the PDP context the RADIUS message is related to. It is encoded as its hexadecimal representation, using 1UTF-8 encoded digit.

11 - 3GPP-***Session Stop Indicator***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 11							
2	3GPP Length= 3							
3	1 1 1 1 1 1 1 1							

3GPP Type: 11

Length: 3

Value is set to all 1.

12 - 3GPP-***Selection-Mode***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 12							
2	3GPP Length= 1							
3	UTF-8 encoded Selection mode string							

3GPP Type: 12

Length: 3

Selection mode value: Text

The format of this attribute shall be a character string consisting of a single digit, mapping from the binary value of the selection mode in the Create PDP Context message (3GPP TS 29.060 [24]). Where 3GPP TS 29.060 [24] provides for interpretation of the value, e.g. map '3' to '2', this shall be done by the GGSN.

13 - 3GPP-***Charging-Characteristics***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 13							
2	3GPP Length= 6							
3-6	UTF-8 encoded Charging Characteristics value							

3GPP Type: 13

Length: 6

Charging characteristics value: Text

The charging characteristics is value is the value of the 2 octets value field taken from the GTP IE described in 3GPP TS 29.060 [24], subclause 7.7.23.

Each octet of this IE field value is represented via 2 UTF-8 encoded digits, defining its hexadecimal representation.

14 - 3GPP-***Charging Gateway IPv6 address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 14							
2	3GPP Length= 18							
3	Charging GW IPv6 addr Octet 1							
4	Charging GW IPv6 addr Octet 2							
5-18	Charging GW IPv6 addr Octet 3-16							

3GPP Type: 14

Length: 18

Charging GW IPv6 address value: IPv6 Address

15 - 3GPP-***SGSN IPv6 address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 15							
2	3GPP Length= 18							
3	SGSN IPv6 addr Octet 1							
4	SGSN IPv6 addr Octet 2							
5-18	SGSN IPv6 addr Octet 3-16							

3GPP Type: 15

Length: 18

SGSN IPv6 address value: IPv6 Address

16 - 3GPP-***GGSN IPv6 address***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 16							
2	3GPP Length= 18							
3	GGSN IPv6 addr Octet 1							
4	GGSN IPv6 addr Octet 2							
5-18	GGSN IPv6 addr Octet 3-16							

3GPP Type: 16

Length: 18

GGSN IPv6 address value: IPv6 Address

17 - 3GPP-***IPv6-DNS-Servers***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 17							
2	3GPP Length= m							
3-18	(1st) DNS IPv6 addr Octet 1-16							
19-34	(2nd) DNS IPv6 addr Octet 1-16							
k-m	(n-th) DNS IPv6 addr Octet 1-16							

3GPP Type: 17

Length: $m = n \times 16 + 2$; $n \geq 1$ and $n \leq 15$; $k = m-15$

IPv6 DNS Server value: IPv6 Address The 3GPP- IPv6-DNS-Servers Attribute provides a list of one or more ('n') IPv6 addresses of Domain Name Server (DNS) servers for an APN. The DNS servers are listed in the order of preference for use by a client resolver, i.e. the first is 'Primary DNS Server', the second is 'Secondary DNS Server' etc. The attribute may be included in Access-Accept packets.

18 - 3GPP-***SGSN MCC-MNC***

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 18							
2	3GPP Length= n							
3	MCC digit1 (UTF-8 encoded)							
4	MCC digit2 (UTF-8 encoded)							
5	MCC digit3 (UTF-8 encoded)							
6	MNC digit1 (UTF-8 encoded)							
7	MNC digit2 (UTF-8 encoded)							
8	MNC digit3 if present (UTF-8 encoded)							

3GPP Type: 18

Length: n shall be 7 or 8 octets depending on the presence of MNC digit 3

SGSN address value: text

This is the UTF-8 encoding of the RAI MCC-MNC values. In accordance with 3GPP TS 23.003 [40] and 3GPP TS 29.060 [24] the MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

16.4.8 Accounting Request Interim-Update (sent from GGSN to AAA server)

Table 8 describes the attributes of the Accounting-Request Interim-Update message.

Table 8: The attributes of the Accounting-Request Interim-Update message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been received in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
4	NAS-IP-Address	IP address of the GGSN for communication with the AAA server.	IPv4	Conditional Notes 1and 3
95	NAS-IPv6-Address	IP address of the GGSN for communication with the AAA server.	IPv6	Conditional Notes 1 and 3
32	NAS-Identifier	Hostname of the GGSN for communication with the AAA server.	String	Conditional Note 1
6	Service-Type	Indicates the type of service for this user	Framed	Optional
7	Framed Protocol	Indicates the type of protocol for this user	7 (GPRS PDP Context)	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 3
97	Framed-IPv6-Prefix	User IPv6 address	IPv6	Conditional Note 3
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 3and 4
25	Class	Received in the access accept	String	Optional (Note 2)
30	Called-Station-Id	Identifier for the target network	APN (UTF-8 encoded)	Mandatory
31	Calling-Station-Id	This attribute is the identifier for the MS, and it shall be configurable on a per APN basis.	MSISDN in international format according to 3GPP TS 23.003 [40], UTF-8 encoded.(Note 6)	Optional
40	Acct-Status-Type	Indicates the type of accounting request	Interim-Update	Mandatory
41	Acct-Delay-Time	Indicates how many seconds the GGSN has been trying to send this record for, and can be subtracted from the time of arrival on the AAA server to find the approximate time of the event generating this Accounting-Request	Second	Optional
42	Acct-Input-Octets	GGSN counted number of octets sent by the user for the PDP context	32 bit unsigned integer	Optional
43	Acct-Output-Octets	GGSN counted number of octets received by the user for the PDP context	32 bit unsigned integer	Optional
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPV6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. (Note 5)	Mandatory
45	Acct-Authentic	Authentication method	RADIUS or	Optional

Attr #	Attribute Name	Description	Content	Presence Requirement
			LOCAL	
46	Acct-Session-Time	Duration of the session	Second	Optional
47	Acct-Input-Packets	GGSN counted number of packets sent by the user	Packet	Optional
48	Acct-Output-Packets	GGSN counted number of packets received by the user	Packet	Optional
61	NAS-Port-Type	Port type for the GGSN	As per RFC 2865 [38]	Optional
26/10415	3GPP Vendor-Specific	Sub-attributes according to subclause 16.4.7.	See subclause 16.4.7	Optional except sub-attribute 3 which is conditional

NOTE 1: Either NAS-IP-Address or NAS-Identifier shall be present.
NOTE 2: The presence of this attribute is conditional upon this attribute being received in the Access-Accept message
NOTE 3: Either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different.
NOTE 4: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.
NOTE 5: GGSN IP address is the same as that used in the GCDRs.
NOTE 6: There are no leading characters in front of the country code.

16.4.9 Disconnect Request (optionally sent from AAA server to GGSN)

Table 9 describes the attributes of the Disconnect-Request message.

Table 9: The attributes of the Disconnect-Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field of the Create PDP Context Request message) or PPP authentication phase (if PPP PDP type is used). If no username is available a generic username, configurable on a per APN basis, shall be present. If the User-Name has been sent in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
8	Framed-IP-Address	User IP address	IPv4	Conditional Note 2
97	Framed-IPv6-Prefix	User IPv6 address	IPv6	Conditional Note 2
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional Notes 1 and 2
44	Acct-Session-Id	User session identifier.	GGSN IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal. (Note 3)	Mandatory

NOTE 1: Included if the prefix alone is not unique for the user. This may be the case, for example, if address is assigned using stateful address autoconfiguration or if a static IPv6 address.
NOTE 2: Either IPv4 or IPv6 address/prefix attribute shall be present.
NOTE 3: The GGSN IP address is the same as that used in the GCDRs.

Annex A (informative): Interworking PCS1900 with PSDNs

Void.

Annex B (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
	Apr 1999				Transferred to 3GPP CN1	7.0.0	
05-1999	TSG#03				Approved at CN#03		3.0.0
06-1999	TSG#04		001		Access to PDNs and ISPs with the PDP-type PPP	3.0.0	3.1.0
06-1999	TSG#04		002		GPRS Internet Hosted Octet Stream Service (IHOSS)	3.0.0	3.1.0
12-1999	TSG#06		003		Clarification on the PPP LCP Negotiation for PDP Type PPP	3.1.0	3.2.0
12-1999	TSG#06		004		Enhancement to Numbering and Addressing to Include the APN	3.1.0	3.2.0
12-1999	TSG#06		005		IPCP Negotiation Interworking at the MT for Non-Transparent IP	3.1.0	3.2.0
12-1999	TSG#06		006		Mobile IP Issues	3.1.0	3.2.0
12-1999	TSG#06		007		Access to an Intranet/ISP with DHCP End to End	3.1.0	3.2.0
12-1999	TSG#06		008		Streamlining	3.1.0	3.2.0
03-2000	TSG#07		009		Specification reference section clean-up	3.2.0	3.3.0
03-2000	TSG#07		010		Support for the IP-Multicast protocol	3.2.0	3.3.0
03-2000	TSG#07		011		Correction for the support of IPv6	3.2.0	3.3.0
03-2000	TSG#07		012		Removal of X.25.	3.2.0	3.3.0
03-2000	TSG#07		013		TSG CN1 Vocabulary Alignment	3.2.0	3.3.0
09-2000	TSG#09		014		Corrections to MobileIP	3.3.0	3.4.0
03-2001	TSG#11	NP-010044	015		DHCP Lease Renewal	3.4.0	3.5.0
03-2001	TSG#11	NP-010044	016		Removal of IHOSS and OSP	3.4.0	3.5.0
03-2001	TSG#11				Upgraded to Release 4	3.5.0	4.0.0
06-2001	TSG#12	NP-010256	018		Clarifications on the non-transparent access mode	4.0.0	4.1.0
06-2001	TSG#12	NP-010256	020		Set the use of PPP between the MT and TE as an option when interworking with MIPv4	4.0.0	4.1.0
09-2001	TSG#13	NP-010530	021	5	Standard method for information delivery (MSISDN; IP address…) between GPRS and external PDN using RADIUS	4.1.0	4.2.0
12-2001	TSG#14	NP-010672	023	2	Standard method for information update between GPRS and external PDN using RADIUS	4.2.0	4.3.0
12-2001	TSG#14	NP-010672	024	2	Standard method for interworking between GPRS and external PDN using RADIUS	4.2.0	4.3.0
12-2001	TSG#14	NP-010572	028	1	Correction to the Calling-Station-Id attribute	4.2.0	4.3.0
12-2001	TSG#14	NP-010572	030	1	Correction to 3GPP Vendor specify attribute 3GPP-IMSI	4.2.0	4.3.0
12-2001	TSG#14	NP-010572	032		Correction to 3GPP vendor specific attributes containing MCC-MNC	4.2.0	4.3.0
03-2002	TSG#15	NP-020080	038		Change of associated attribute for 3GPP-NSAPI	4.3.0	4.4.0
06-2002	TSG#16	NP-020295	048	1	Corrections to the 3GPP RADIUS attributes	4.4.0	4.5.0
06-2002	TSG#16	NP-020295	055	3	Clarification on the Radius Flows	4.4.0	4.5.0
06-2002	TSG#16	NP-020171	060		Address autoconfiguration of IPv6 terminals and IPv6 update	4.4.0	4.5.0
12-2002	TSG#18	NP-020613	065		Correction of figure for Radius Accounting Update	4.5.0	4.6.0
12-2002	TSG#18	NP-020614	069		Corrections related to IPv6	4.5.0	4.6.0
12-2002	TSG#18	NP-020613	071		RADIUS enhancement for identification of VPLMN	4.5.0	4.6.0
12-2002	TSG#18	NP-020613	071		RADIUS enhancement for identification of VPLMN	4.5.0	4.6.0
03-2003	TSG#19	NP-030074	082	1	Correction of References and specification Corrections	4.6.0	4.7.0
06-2003	TSG#20	NP-030199	085	1	Configuration of Domain Name System (DNS) server IPv6 addresses	4.7.0	4.8.0
06-2003	TSG#20	NP-030200	090	1	Attribute corrections	4.7.0	4.8.0
12-2003	TSG#22	NP-030563	097	1	Updated reference for DHCPv6	4.8.0	4.9.0

History

Document history		
V4.0.0	March 2001	Publication
V4.1.0	June 2001	Publication
V4.2.0	September 2001	Publication
V4.3.0	December 2001	Publication
V4.4.0	March 2002	Publication
V4.5.0	June 2002	Publication
V4.6.0	December 2002	Publication
V4.7.0	March 2003	Publication
V4.8.0	June 2003	Publication
V4.9.0	December 2003	Publication